Journal of Algebra 322 (2009) 675–702

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

An algorithm for Lang's Theorem ☆

Arjeh M. Cohen [a,*], Scott H. Murray [b]

[a] Eindhoven University of Technology, Department of Mathematics and Computer Science, PO Box 513, Eindhoven, Netherlands
[b] Department of Mathematics and Statistics F07, University of Sydney, NSW 2006, Australia

ARTICLE INFO

Article history:
Received 6 June 2005
Available online 25 April 2009
Communicated by William M. Kantor

To John Cannon and Derek Holt on the occasions of their significant birthdays, in recognition of distinguished contributions to mathematics

Keywords:
Lie algebra
Linear algebraic group
Chevalley basis
Weyl group
Derangements
Las Vegas type algorithm
Maximal toral subalgebra

ABSTRACT

We give an efficient Las Vegas type algorithm for Lang's Theorem in split connected reductive groups defined over finite fields of characteristic greater than 3. This algorithm can be used to construct many important structures in finite groups of Lie type. We use an algorithm for computing a Chevalley basis for a split reductive Lie algebra, which is of independent interest. For our time analysis we derive that the proportion of reflection derangements in a Weyl group is less than 2/3.

1. Introduction

A finite group of Lie type can be described as the rational points of a connected reductive algebraic group over a finite field. Given a structure in the algebraic group, such as a conjugacy class or a maximal torus, we want to find the corresponding structures in the finite group of Lie type. This can often be achieved with Lang's Theorem. We provide a computationally efficient algorithm for Lang's Theorem in split connected reductive groups. Our algorithm is randomised but guaranteed to return

☆ The authors would like to thank Sergei Haller, Anthony Henderson, William M. Kantor, Gus Lehrer, Dan Roozemond, T.A. Springer, and D.E. Taylor for useful discussions on this topic. The authors also thank the Magma project at the University of Sydney, where some of the work was carried out.

* Corresponding author.
E-mail address: a.m.cohen@tue.nl (A.M. Cohen).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.04.013

a correct answer, i.e., it is Las Vegas in the sense of [Bab97]. We have implemented this algorithms in the Magma computer algebra system [BC97]. Glasby and Howlett [GH97] have already solved this problem in a special case; our algorithm is inspired by their work and the proof of Lang's Theorem given in [Mül03].

Throughout this paper, k is a finite field of size q and characteristic p, and k_r is the unique degree r extension of k in the algebraic closure $\bar{k}$. The affine space of dimension N can be identified with $\bar{k}^N$. An *affine variety* X is a subset of $\bar{k}^N$ that consists of the zeroes of a collection of polynomials. The variety is *defined over* k if it is closed under the action of the map $F : \bar{k}^N \to \bar{k}^N$ that takes the qth power of each component. The restriction of F to X is called the (*standard*) *Frobenius endomorphism* of X. The set of *rational points* of X over k_r, denoted by $X(k_r)$, consists of those elements of X fixed by F^r. A *nonstandard Frobenius endomorphism* is a morphism $F' : X \to X$ such that $(F')^s = F^s$ for some positive integer s. The elements of X fixed by F' are the rational points of a *k-form* of X. In this paper, Frobenius endomorphisms are standard unless otherwise stated.

A *linear algebraic group* is an affine variety with group multiplication and inversion given by rational functions. See, for example, [Spr98] for more details including the definitions of reductive and connected groups. Every linear algebraic group contains a maximal connected subgroup G°, the component of the identity. This subgroup is normal and G/G° is finite, so for many purposes it suffices to study connected groups. An important result on linear algebraic groups over finite fields is

Theorem 1.1 *(Lang's Theorem). If G is a connected linear algebraic group defined over the finite field k with Frobenius map F, then the map*

$$G \to G, \quad a \mapsto a^{-F}a$$

is onto.

This is equivalent to the statement that the first Galois cohomology of G is trivial.

In this paper, we give an algorithm for Lang's Theorem for G a k-split connected reductive group. This is likely to be the critical case for an algorithm for arbitrary connected algebraic groups (see Section 3). The group G is determined by the base field k and a root datum $(X, \Phi, Y, \Phi^\star)$ [Dem65]. We describe G by the Steinberg presentation with generators $x_\alpha(a)$, for $\alpha \in \Phi$ a root and $a \in k$, and $y \otimes t$, for $y \in Y$ and $t \in k^\times$. The relations are given in [CMT04, Section 4.1]. The action of the standard Frobenius map is given by $x_\alpha(a)^F = x_\alpha(a^q)$ and $(y \otimes t)^F = y \otimes t^q$.

Recall that the (reductive) rank n of G is the rank of X and the semisimple rank ℓ of G is the rank of the root system Φ. The *fundamental group* of G is the quotient of the full integer lattice $\mathbb{Z}^\ell$ by the sublattice generated by the rows of the Cartan matrix. This group is finite and depends only on the Cartan type of G. If G is simple of Cartan type A_ℓ, then the fundamental group is cyclic of order $\ell + 1$; for all other simple groups, the fundamental group has order at most 4.

We use soft-O notation to simplify our timings: recall that $O^\sim(N)$ means $O(N(\log(N))^c)$ for some constant c. Addition, subtraction, multiplication, division, and equality testing in the field of size q all take time $O^\sim(\log(q))$ by [Shp99, Introduction]. In [CHM08], we showed that elements of G can be stored as *canonical words* of length $O(n + \ell^2)$; and multiplication and inversion of elements in $G(k)$ takes time $O^\sim(n^3 \log(q))$.

We can now state our main result:

Theorem 1.2. *Let k be a finite field of size q and of characteristic greater than 3. Let G be a k-split connected reductive linear algebraic group of rank n. Let m be the exponent of the fundamental group of G. Let c be in $G(k_r)$, and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Then we can find $a \in G(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O^\sim(n^9 m^2 r^2 s^2 \log(q)^2)$.*

We can improve significantly on this result for simple classical groups:

Theorem 1.3. *Let G be a k-split simple classical group of rank n, defined over the field k of size q. Let m be the exponent of the fundamental group of G. Let c be in $G(k_r)$ and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Then we can find $a \in G(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O^\sim(n^3m^2r^2s^2\log(q)^2)$.*

Note that a similar timing also applies to simple exceptional groups when q has characteristic greater than 3, since the rank is bounded.

The parameter s measures the size of the field extension required, as explained in Section 2. The input element c has size $O^\sim(n^2r\log(q))$ and the output element a has size $O^\sim(n^2rs\log(q))$. So our running time is polynomial in the size of the output rather than the input. In Section 3, we use the concept of F-eigenvectors to reduce to a problem involving forms of G-modules. A solution to this problem and a proof of Theorem 1.3 is given in Section 4.2. This solution uses the algorithm for computing a standard Chevalley basis in the Lie algebra of G described in Section 5.

The key result in obtaining the Chevalley basis may be of interest in its own right and so we state it here.

Theorem 1.4. *Suppose that k is a finite field of size q and characteristic greater than 3. Let G be a k-split connected reductive group and let L be the Lie algebra of G. We can find a split maximal toral subalgebra of L in Las Vegas time $O^\sim(n^9\log(q)^2)$.*

Note that this is equivalent to time $O^\sim(d^{4.5}\log(q)^2)$, where d is the dimension of L. This is similar to a result by Ryba [Ryb07].

The running times of the algorithms are analysed in Section 6, leading to proofs of Theorems 1.2 and 1.4. This uses an interesting extension of a standard result from combinatorics. Recall that a permutation is called a *derangement* if it has no fixed points. The proportion of derangements in the symmetric group Sym_t acting on t letters is known to approach $1/e$ as $t \to \infty$. We give a similar result for Weyl groups acting by conjugacy on reflections:

Theorem 1.5. *The proportion of derangements in a Weyl group acting on reflections is less than $2/3$.*

2. Minimum field degree

Computation in large finite fields is a challenging problem (see, for example, [LN97]). So we start with an easy result giving the size of the field extension needed for Lang's Theorem. We define the *minimum field degree* of $g \in G$ as the smallest r such that $g^{F^r} = g$. Note that g has minimum field degree r if, and only if, k_r is the smallest extension of k such that g is in $G(k_r)$. The minimal field degree of g can be computed by finding the smallest field k_r containing all the field elements occurring in the canonical word for g.

We can now determine the minimal field degree of the output of our algorithm:

Proposition 2.1. *Let G be a connected linear algebraic group defined over k. Let c be an element of G with minimum field degree r and let s be the order of $c^{F^{r-1}} \cdots c^F c$. If $c = a^{-F}a$ for some a in G, then the minimum field degree of a is rs.*

Proof. Let m be the minimum field degree of a. Clearly k_r is a subfield of k_m, so r is a divisor of m, say $ru = m$. Since $c^{F^r} = c$, we have

$$\left(c^{F^{r-1}} \cdots c^F c\right)^u = c^{F^{m-1}} \cdots c^F c = a^{-F^m} a^{F^{m-1}} \cdots a^{-F^2} a^F a^{-F} a = a^{-F^m} a.$$

Hence $a^{F^m} = a$ if, and only if, u is a multiple of s. □

The most important consequence of this proposition is that the minimum field degree is independent of the particular choice of a and can be computed beforehand. In all our timings of algorithms with input c, we consider s, the order of $c^{F^{r-1}} \cdots c^F c$, to be an input of our algorithm. While it is

```
LANG := function(G, c, s)        [(c^{F^{r-1}} ··· c^F c)^s = 1 where c ∈ G(k_r)]
  construct a module V for G
  let E(k) = F-EIGENSPACE(c, V, s)
  find a transformer a ∈ G(k_rs) for E
  if V is faithful then
    return a
  else
    construct a connected k-subgroup H < G containing the kernel of V
    let b = LANG(H, a^F c a^{-1}, s)
    return ba
  end if
end function
```

Algorithm 1. Algorithm outline for Lang's Theorem.

straightforward to compute s, no polynomial time algorithm is known. The best known method for computing s is to convert from the Steinberg presentation of G to a faithful representation [CMT04] and then compute the order of the corresponding matrix using the Las Vegas algorithm of [CLG97]. If d is the degree of our matrix, this algorithm takes time $O^{\sim}(d^3 \log(q))$, plus the time required to factor a collection of integers of the form $q^{d_i} - 1$ with $\sum_i d_i \leqslant d$.

Suppose now that G is a k-split reductive group with reductive rank n and semisimple rank ℓ. The element c, which is the input to our algorithm, has size $O^{\sim}((n + \ell^2) r \log(q))$; while the element a, which is the output, has size $O^{\sim}((n+\ell^2) rs \log(q))$. Since s need not be bounded by a polynomial in n, ℓ, r, and $\log(q)$, there is no algorithm for Lang's Theorem that is polynomial in the size of the input. The best we can hope for is an algorithm which is polynomial in the size of the output. We note that s can be quite small in practise. For example, to construct twisted tori we need to apply Lang's Theorem to Weyl group representatives (the elements denoted $\dot{w}$ in the Steinberg presentation). These elements have $r = 1$ and s at most $O(\ell^2)$.

3. Twisted eigenvectors

Let $V = \bar{k}^d$ be a *split* vector space defined over k, so that F acts on $V = \bar{k}^d$ by taking the qth power of each component. We say that $v \in V$ is an *F-eigenvector* of $c \in \mathrm{GL}_d(\bar{k})$ if $v^F c = v$ (note that the "F-eigenvalue" is always one). The set $E(k)$ of all F-eigenvectors in V is a k-space of dimension d. Once again take r to be the minimum field degree of c, and s to be the order of $c^{F^{r-1}} \cdots c^F c$. By Lang's Theorem, the k_{rs}-span of $E(k)$ must be equal to $V(k_{rs})$. There is a variety E defined over k such that $E(k_t)$ is the k_t-span of $E(k)$ for every positive integer t. Such a variety is called a *k-form* of V [Spr98, Section 11.1].

The following easy lemma is the key to our recursive approach.

Lemma 3.1. *Let G be a connected linear algebraic group defined over k and let V be a G-module defined over k with kernel $K \leqslant G$. Let c be an element of G. Suppose that $E(k)$ is the set of F-eigenvectors of c in V. Then $a \in G$ satisfies $c \in a^{-F} K a$ if, and only if, $V(k)a = E(k)$.*

Proof. If $a^{-F} z a = c$ for $z \in K$, then, for all $v \in V(k)$, $va = vza = va^F c = (va)^F c$ and so $va \in E(k)$. Conversely, if $V(k)a = E(k)$, then, for all $v \in V(k)$, $va = (va)^F c = va^F c$ and so $a^F c a^{-1} \in K$. □

Our approach to solving Lang's Theorem is outlined in Algorithm 1. We call an element $a \in G(k_{rs})$ such that $V(k)a = E(k)$ a *transformer* in G for the k-form E. If V is faithful, then the previous lemma ensures that $a^{-F} a = c$. Otherwise we recurse to a connected subgroup containing the kernel K. Note that s is taken to be the order of $c^{F^{r-1}} \cdots c^F c$ in the top-level function call. It is not necessary to recompute s for the recursive calls since a multiple of the element order works just as well.

Suppose now that G is a split connected reductive group described by a Steinberg presentation. Let T_0 be the subgroup generated by the elements $y \otimes t$, for $y \in Y$ and $t \in \mathbb{F}^{\times}$. Then T_0 is the *standard* k-split maximal torus of G. Using the methods of [CMT04], we can construct a module V which is *projectively faithful*, that is, the kernel K is contained in the centre $Z(G)$ of G. We can now

F-EIGENSPACE := **function**(c, V, s) $\quad [(c^{F^{r-1}} \cdots c^F c)^s = 1$ where $c \in \mathrm{GL}(V(k_r))]$
  let S be the k-matrix of F acting of k_{rs}
  let C be the k-matrix of c acting on $V(k_{rs}) = k_{rs}^d$
  return the fixed point space of $S^{\oplus d} C$
end function

Algorithm 2. Deterministic method for computing F-eigenspaces.

F-EIGENSPACE := **function**(c, V, s) $\quad [(c^{F^{r-1}} \cdots c^F c)^s = 1$ where $c \in \mathrm{GL}(V(k_r))]$
  repeat
    let x be a random $d \times d$ matrix over k_{rs}
    let $a = x + x^F c + x^{F^2} c^F c + \cdots + x^{F^{rs-1}} c^{F^{rs-2}} \cdots c^F c$
  until a is invertible
  return $V(k)a^{-1}$
end function

Algorithm 3. Las Vegas method for computing F-eigenspaces.

take $H = T_0$ in Algorithm 1, since $Z(G)$ is contained in every maximal torus of G. Since a split torus has an easily constructed faithful module, there is at most one recursive call for reductive groups. The same algorithm could, in principle, be used for a nonreductive connected group G: construct a reductive quotient G/N, take V to be the G-module induced by a projectively faithful module for G/N, and take H to be the preimage in G of the maximal torus in G/N. However, finding the normal subgroup N and constructing the quotient G/N are nontrivial problems which lie beyond the scope of this paper.

Algorithms for finding transformers are discussed in the next section. We now give two algorithms for computing the F-eigenspace. The most straightforward method is given in Algorithm 2. The key is to consider k_{rs} as a k-space of dimension rs and to consider $V(k_{rs}) = k_{rs}^d$ as a k-space of dimension drs. The solution is then found by linear algebra over k. We compute S in time $O^\sim(r^2 s^2 \log(q)^2)$ by taking qth powers of the elements in a k-basis of k_{rs}. Finding C takes time $O^\sim(r^2 s^2 \log(q))$. The fixed space computation takes time $O^\sim(d^3 r^3 s^3 \log(q))$. So the overall algorithm requires time $O^\sim(d^3 r^3 s^3 \log(q)^2)$.

An alternative method, due to Glasby and Howlett [GH97], is given in Algorithm 3. It takes time $O^\sim(d^2 rs \log(q)^2)$ to apply F to a $d \times d$ matrix, so computing a takes time $O^\sim(d^3 r^2 s^2 \log(q)^2)$. Each randomly chosen x has a probability of at least $1/4$ of yielding an invertible element a. Since this probability is bounded away from zero as q, r, s, and d become large, the algorithm is Las Vegas. Note that we have an algorithm for Lang's Theorem for the case $G = \mathrm{GL}(V)$ if the function returns a instead of $V(k)a^{-1}$.

We now have

Theorem 3.2. *Let V be a split vector space over k with dimension d. Let c be an element of $\mathrm{GL}(V)$ with minimum field degree r and let s be the order of $c^{F^{r-1}} \cdots c^F c$. We can compute a basis for the k-space $E(k)$ of F-eigenvectors of c in deterministic time $O^\sim(d^3 r^3 s^3 \log(q)^2)$ or Las Vegas time $O^\sim(d^3 r^2 s^2 \log(q)^2)$.*

4. Finding transformers

Let G be a k-split connected reductive linear algebraic group defined over k. Suppose that G is described by the Steinberg presentation with root datum (X, Φ, Y, Φ^*). Let c be in $G(k_r)$, and let s be the order of $c^{F^{r-1}} \cdots c^F c$. Let V be a projectively faithful G-module and compute E, the k-form of F-eigenvectors of c. In this section, we show how to find a transformer $a \in G(k_{rs})$ such that $E(k)a = V(k)$. First we consider two special cases: k-split tori and classical groups. Then we give an algorithm for an arbitrary k-split connected reductive group. The key is to consider bases of $V(k)$ with some additional structure that ensures that G is transitive on all such bases (or G_{ad} is transitive in Section 4.3).

4.1. Split tori and isogeny

A *k-split torus* T of dimension n is the split connected reductive group with root datum $(\mathbb{Z}^n, \emptyset, \mathbb{Z}^n, \emptyset)$. So T is just $\mathbb{Z}^n \otimes \bar{k}^\times = (\bar{k}^\times)^n$ with the Frobenius endomorphism taking the qth power of each component. The standard module V is just $\bar{k}^n$ with the componentwise action. Suppose $c = (c_1, \ldots, c_n) \in T(k_r)$ and E is the variety of F-eigenvectors of c in V. Applying Theorem 3.2 to each component separately, we can compute E in Las Vegas time $O^\sim(nr^2s^2\log(q)^2)$. This gives a basis of E of the form $a_1e_1, \ldots, a_ne_n$ where each $a_i \in k_{rs}^\times$ and e_i is the ith standard basis vector in V. Now $(a_1, \ldots, a_n) \in T(k_{rs})$ is a transformer for E. Hence we have proved

Proposition 4.1. *Let T be a k-split torus of dimension n. Let c be in $T(k_r)$, and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Then we can find an element a in $T(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O^\sim(nr^2s^2\log(q)^2)$.*

We now give an application of this proposition to isogenous groups. Consider two split connected reductive groups G_1 and G_2 defined over k. Let $(X_i, \Phi_i, Y_i, \Phi_i^\star)$ be the root datum of G_i for $i = 1, 2$. Suppose that there is an isomorphism $\phi : Y_1 \otimes \mathbb{Q} \to Y_2 \otimes \mathbb{Q}$ such that $\phi(Y_1) \subseteq Y_2$ and $\phi(\Phi_1^\star) = \Phi_2^\star$. For $\alpha \in \Phi_1$, define $\bar{\alpha} \in \Phi_2$ by $\phi(\alpha^\star) = \bar{\alpha}^\star$.

We can easily modify the presentation of G_2 so that the signs defined in [CMT04, Section 2] agree (i.e., $\epsilon_{\alpha\beta} = \epsilon_{\bar{\alpha}\bar{\beta}}$ for all $\alpha, \beta \in \Phi_1$). Then $\iota : G_1 \to G_2$ defined by

$$\iota\big(x_\alpha(a)\big) = x_{\bar{\alpha}}(a) \quad \text{and} \quad \iota(y \otimes t) = \phi(y) \otimes t$$

is an *isogeny*, i.e., an epimorphism with finite kernel. Every isogeny from a split connected reductive group G_1, with kernel contained in the centre of G_1, can be put in this form by precomposing with an automorphism of G_1 [Car93]. Denote by T_i the standard torus $Y_i \otimes \bar{k}^\times$. Note that the kernel K of ι is a finite subgroup of $Z(G_1) \leqslant T_1$. An important invariant of ι is the exponent of K, which we denote by m. Note that m is bounded by the exponent of the fundamental group of G_1 (or G_2, since the groups have the same Cartan matrix).

For $g \in T_1(k_r)$, we have $\iota(g)^{F^r} = \iota(g^{F^r}) = \iota(g)$, so $\iota(g) \in T_2(k_r)$. This image can be computed in time $O^\sim(n^3r\log(q))$ by linear algebra over k_r.

For $h \in T_2(k_r)$, we can find $g \in T_1$ such that $\iota(g) = h$. Then $\iota(g^{-F^r}g) = h^{-F^r}h = 1$, i.e., $g^{-F^r}g \in K$. Hence $(g^{-F^r}g)^m = 1$ and so $g^m \in T_1(k_r)$. Using the fact that T_0 is a direct sum of copies of $\bar{k}^\times$, such a g must be in $T_0(k_{rm})$. This preimage can be computed in time $O^\sim(n^3rm\log(q))$.

Proposition 4.2. *Let G_1 and G_2 be k-split connected reductive linear algebraic groups defined over k with reductive rank n. Suppose we have an isogeny $\iota : G_1 \to G_2$, defined as above, whose kernel has exponent m. For c in G_1 or G_2, let $s(c)$ denote the order of $c^{F^{r-1}} \cdots c^F c$, where r is the minimum field degree of c.*

1. *Lang's Theorem can be solved for $c \in G_1(k_r)$ in time $O^\sim(n^3r^2s(c)^2m^2\log(q)^2)$, plus the time needed to solve it for some $c' \in G_2(k_r)$ with $s(c') \leqslant s(c)$.*
2. *Lang's Theorem can be solved for $c \in G_2(k_r)$ in time $O^\sim(n^3rs(c)m^2\log(q))$, plus the time needed to solve it for some $c' \in G_1(k_{rm})$ with $s(c') \leqslant ms(c)$.*

Proof. If $c \in G_1(k_r)$, then $c' = \iota(c)$ can be found in time $O^\sim(n^3r\log(q))$. Clearly $s(c') \leqslant s(c)$. Now we can find $a' \in G_2(k_{rs(c)})$ such that $a'^{-F}a' = c'$. Let $a \in G_1(k_{rsm})$ be a preimage of a' computed in time $O^\sim(n^3rm\log(q))$. Consider $a^F ca^{-1} \in K(k_{rs(c)m}) \leqslant T_1(k_{rs(c)m})$. Now

$$\big(a^F ca^{-1}\big)^{F^{rs(c)m-1}} \cdots \big(a^F ca^{-1}\big)^F \big(a^F ca^{-1}\big) = a^{F^{rs(c)m}}\big(c^{F^{rs(c)m-1}} \cdots c^F c\big)a^{-1} = 1.$$

So by Proposition 4.1, we can find $b \in T_1(k_{rs(c)m})$ such that $a^F ca^{-1} = b^{-F}b$ in Las Vegas time $O^\sim(nr^2s(c)^2m^2\log(q)^2)$. Now $(ba)^{-F}ba = c$ and Part (1) follows.

If $c \in G_2(k_r)$, we can find an element $c' \in G_1(k_{rm})$ such that $\iota(c') = c$ in time $O^\sim(n^3 mr \log(q))$. Since $(c'^{F^{r-1}} \cdots c'^F c')^{s(c)} \in k_m$, we get $s(c')|ms(c)$. We can now find $a' \in G_2(k_{rs(c)m^2})$ such that $c' = a'^{-F} a'$. Then $a = \iota(a')$ can be computed in time $O^\sim(n^3 rs(c)m^2 \log(q))$ and $a^{-F} a = c$. □

Let G be a split connected reductive group with root datum $(X, \Phi, Y, \Phi^\star)$. Define $Y_{\mathrm{sc}} = \mathbb{Z}\Phi^\star$ and let X_{sc} be its dual lattice in $X \otimes \mathbb{Q}$. Then $(X_{\mathrm{sc}}, \Phi, Y_{\mathrm{sc}}, \Phi^\star)$ is also a root datum, with corresponding group denoted G_{sc}. There is an isogeny map $G_{\mathrm{sc}} \to G$ induced by the embedding $Y_{\mathrm{sc}} \to Y$. Note that G_{sc} is simply connected if G is semisimple. A dual construction gives us a group G_{ad}, which is adjoint when G is semisimple, and an isogeny $G \to G_{\mathrm{ad}}$. It is well known that the action of G_{ad} on the corresponding Lie algebra is faithful. In light of the above proposition, an effective algorithm for Lang's Theorem need only find a transformers for adjoint groups.

4.2. Classical groups

We now show how to find transformers for the classical groups, using the standard representations. See [CHM08] for the relationship between these representations and the Steinberg presentations. Throughout this section we take $V = \bar{k}^d$ and B_0 to be the standard basis $e_1, \ldots, e_d$ of $V(k)$.

The easiest case is $G = \mathrm{GL}_d(\bar{k})$: Let B be a k-basis of $E(k)$. Let a be the matrix whose rows are the elements of B. Then $B_0 a = B$, and so a is a transformer for E.

Now suppose $G = \mathrm{SL}_d(\bar{k})$. Given a basis B of V, define its *volume*, denoted $\mathrm{vol}(B)$, to be the determinant of the matrix whose rows are the elements of B. Then B_0 has volume one and G is transitive on all bases of volume one. Now suppose B is a basis of $E(k)$, the set of F-eigenvectors of $c \in G$. Then $B^F c = B$, so

$$\mathrm{vol}(B)^F = \mathrm{vol}\big(B^F\big) = \mathrm{vol}\big(Bc^{-1}\big) = \mathrm{vol}(B)\det(c)^{-1} = \mathrm{vol}(B),$$

and so $\mathrm{vol}(B) \in k$. We can now construct a basis B' of $E(k)$ with volume one by dividing the first element of B by the scalar $\mathrm{vol}(B)$. So the matrix that takes B_0 to B' is a transformer in G.

Now suppose that q is odd. Let M be an orthogonal or symplectic form on V whose value is written (u, v) for $u, v \in V$. Further suppose that M is defined over k. Then the invariant group

$$G = \big\{ x \in \mathrm{GL}_d(\bar{k}) \;\big|\; (ux, vx) = (u, v) \big\}$$

is a reductive linear algebraic group defined over k. Note that G is not necessarily split or connected however. Let δ be a fixed nonsquare in k. Define the $m \times m$ matrix

$$A_m = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}.$$

Then the form M has precisely one of the following Gram matrices M_B with respect to some basis B:

- If M is orthogonal and $d = 2\ell + 1$, then

$$M_B = A_d \quad \text{or} \quad \begin{pmatrix} & & A_\ell \\ & \delta & \\ A_\ell & & \end{pmatrix}.$$

```
NormalBasis := function(U)
  let u be a nonzero element of U
  if dim(U) = 1 then
    find a ∈ k such that a^2 = (u,u) or a^2 δ = (u,u)
    return u/a
  end if
  let v be a nonzero element of u^⊥ \ ku
  if dim(U) = 2 then
    if (u,u) ∈ −δ(v,v)k^×2 then      [U anisotropic]
      find a, b ∈ k such that (u,u)a^2 + (v,v)b^2 = 1
      find c ∈ k such that ((u,u)a^2 − (v,v)b^2)c^2 = −δ
      return au + bv, c(au − bv)
    else      [U isotropic]
      find a, b ∈ k such that (u,u)a^2 + (v,v)b^2 = 0
      let w be a nonzero element of (au + bv)^⊥
      return au + bv, w
    end if
  end if
  let w be a nonzero vector in (ku + kv)^⊥ \ (ku + kv)
  find a, b, c ∈ k such that (u,u)a^2 + (v,v)b^2 + (w,w)c^2 = 0
  let x be a nonzero element of (au + bv + cw)^⊥
  return au + bv + cw, NormalBasis({u,v}^⊥), x
end function
```

Algorithm 4. Finding a normal basis for a space with a bilinear form.

- If M is orthogonal and $d = 2\ell$, then

$$M_B = A_d \quad \text{or} \quad \begin{pmatrix} & & & A_{\ell-1} \\ & & 1 & \\ & -\delta & & \\ A_{\ell-1} & & & \end{pmatrix}.$$

- If M is symplectic, then $d = 2\ell$ and

$$M_B = \begin{pmatrix} & A_\ell \\ -A_\ell & \end{pmatrix}.$$

A *normal basis* for M is a basis of V such that M_B is one of these matrices.

Given a symplectic or orthogonal form M on the k-space U, Algorithm 4 constructs a normal basis for U. The quadratic equations involved always have solutions by the standard classification theory of bilinear forms over finite fields (see [Gro02] for more details). Each of these equations can be solved in Las Vegas time $O^\sim(\log(q)^2)$ by [vzGS92]. Note that this construction is rational (that is, it does not use extensions of k) and takes time $O^\sim(d^3\log(q) + d\log(q)^2)$.

If the form M is symplectic, we are done: our transformer is simply the matrix taking a normal basis of $V(k)$ to a normal basis of $E(k)$.

If M is orthogonal, the two normal bases may have different Gram matrices, in which case the equation in Lang's Theorem has no solution. This is to be expected, since G is not connected in this case. If we take $G = \mathrm{SO}_d(M)$, then this problem can be avoided. Without loss of generality, the standard basis B_0 is normal. Suppose that B is a normal basis of $E(k)$. As with the special linear group, $\mathrm{vol}(B)$ is in k. Also

$$\det(M_B) = \det\bigl(BM_{B_0}B^T\bigr) = \mathrm{vol}(B)^2\det(M_{B_0}).$$

But the two choices given above for the Gram matrix have determinants in different cosets of $k^{\times 2}$, hence $M_{B_0} = M_B$. It now remains to ensure that $\mathrm{vol}(B)$ is one. Now $\mathrm{vol}(B)^2 = \det(M_{B_0})/\det(M_B) = 1$,

so suppose $\mathrm{vol}(B) = -1$. If $M_B = A_d$, then exchanging the first and last vectors in B results in a new normal basis with volume one. Otherwise, negating the $(\ell+1)$st vector in B has the same effect.

Similar methods work for quadratic forms in characteristic two. Using the Las Vegas algorithm of Theorem 3.2 to find a basis for $E(k)$, we now have

Proposition 4.3. *Let G be $\mathrm{GL}_d(\bar{k})$, $\mathrm{SL}_d(\bar{k})$, $\mathrm{Sp}_d(M)$ for some symplectic form M, or $\mathrm{SO}_d(M)$ for some orthogonal or quadratic form M. Let c be an element of G with minimum field degree r and let s be the order of $c^{F^{r-1}} \cdots c^F c$. Then we can find $a \in G(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O^\sim(d^3 r^2 s^2 \log(q)^2)$.*

Note that this result applies to nonsplit special orthogonal groups, and could easily be extended to the unitary groups as well.

We can now prove Theorem 1.3: Let G be a split simple classical group G of (reductive and semisimple) rank n. Then G is isogenous to one of the groups considered above, with $d = O(n)$.

If G has type A_n, then there is an isogeny map $\mathrm{SL}_{n+1}(\bar{k}) \to G$ with $m \leqslant n+1$. We can easily ensure that this map is defined with respect to the Steinberg presentation as in the previous section. By Proposition 4.2(2), we can solve Lang's Theorem in G in Las Vegas time $O^\sim(n^3 m^2 r^2 s^2 \log(q)^2)$.

If G is of type B_n, C_n, or D_n, then let G_{sc} be the simply connected group with the same Cartan type as G. We can find isogenies $G_{\mathrm{sc}} \to G$ and $G_{\mathrm{sc}} \to H$ as in the previous section, where H is either $\mathrm{SO}_{2n+1}(M)$, $\mathrm{Sp}_{2n}(M)$, or $\mathrm{SO}_{2n}(M)$ for the appropriate form M. For each of these isogenies, m is at most 4. So, by Proposition 4.2, we can solve Lang's Theorem in Las Vegas time $O^\sim(n^3 r^2 s^2 \log(q)^2)$.

The exceptional groups can also be described as invariant groups of multilinear structures. We could find transformers for these group by normalising the corresponding structures. Examples include composition algebras for groups of type G_2 and Jordan algebras for groups of type F_4 [SV00].

4.3. Adjoint representation

Now consider an arbitrary k-split connected reductive linear algebraic group G, with reductive rank n and semisimple rank ℓ. Then G is given by the Steinberg presentation with root datum $(X, \Phi, Y, \Phi^\star)$ and standard k-split maximal torus $T_0 = Y \otimes \bar{k}^\times$. Fix dual bases $e_1, \ldots, e_n$ for X and $f_1, \ldots, f_n$ for Y. The Lie algebra $L = L(G)$ is a G-module defined over k. This is called the *adjoint representation* of G and it is projectively faithful. Now $L(k)$ has basis elements e_α for $\alpha \in \Phi$ and $h_i \in L(T_0)$ for $i = 1, \ldots, n$ with structure constants:

$$[h_i, h_j] = 0, \tag{1}$$

$$[e_\alpha, h_i] = \langle \alpha, f_i \rangle e_\alpha, \tag{2}$$

$$[e_{-\alpha}, e_\alpha] = \sum_{i=1}^{n} \langle e_i, \alpha^\star \rangle h_i, \tag{3}$$

$$[e_\alpha, e_\beta] = \begin{cases} N_{\alpha\beta} e_{\alpha+\beta} & \text{for } \alpha+\beta \in \Phi, \\ 0 & \text{for } \alpha+\beta \notin \Phi,\ \beta \neq -\alpha, \end{cases} \tag{4}$$

where the integral constants $N_{\alpha\beta}$ are defined in [Car72]. Such a basis is called a *Chevalley basis*. Computing the structure constants as in [CMT04,CHM08], we can construct $L(G)$ from the root datum in time $O^\sim((n+\ell^2)^3 \log(q))$. The action of G on L is given by

$$h_i(y \otimes t) = h_i, \qquad h_i x_\alpha(a) = h_i + \langle \alpha, f_i \rangle a e_\alpha,$$

$$e_\beta(y \otimes t) = t^{\langle \beta, y \rangle} e_\beta, \qquad e_\beta x_\alpha(a) = \sum_{i=1}^{q_{\alpha\beta}} M_{\alpha\beta i} a^i e_{i\alpha+\beta},$$

with $q_{\alpha\beta}$ and $M_{\alpha\beta i}$ as defined in [CMT04].

Choose simple roots $\alpha_1, \ldots, \alpha_\ell$, and fix a linear ordering $<$ on Φ^+ which is compatible with height, i.e., $\mathrm{ht}(\alpha) < \mathrm{ht}(\beta)$ implies that $\alpha < \beta$. Given a nonsimple positive root ξ, take the positive roots α, β such that $\xi = \alpha + \beta$ and α is as small as possible with respect to the ordering on Φ^+. We call (α, β) the *extraspecial pair* of ξ. We can choose a Chevalley basis of L so that the integers $N_{\alpha\beta}$ are positive on extraspecial pairs by [Car72]. We call such a basis a *standard Chevalley basis*. Note that, as with the normal bases in Section 4.2, the problem of finding a standard Chevalley basis is rational over k.

The linear map a taking the standard Chevalley basis of $L(k)$ to a standard Chevalley basis of $E(k)$ must be an automorphism of $L(k_{rs})$. We now need to find a transformer in G. Define G_{ad} as in Section 4.1 and let Γ be the automorphism group of the Dynkin diagram of G. For each element of Γ, fix a graph automorphism normalising both T_0 and the Borel subgroup determined by Φ^+, as in [Car72]. If the characteristic of k is greater than 3, then it follows from [Hog82] that

$$\mathrm{Aut}\big(L(k_{rs})\big) \cong C\big(\Gamma \ltimes G_{\mathrm{ad}}(k_{rs})\big),$$

where C is the pointwise stabiliser of $(Z(L) \cap [L, L])(k_{rs})$ inside $\mathrm{GL}(Z(L)(k_{rs}))$. We can compute a decomposition $a = z\gamma b$ with $z \in C$, γ a graph automorphism, and $b \in G_{\mathrm{ad}}(k_{rs})$ in $O(d^3)$ operations over k_{rs} using a slight modification of Algorithm 6 of [CMT04]. Since $L(k)z\gamma = L(k)$, the element b is a transformer in G_{ad}. The dimension of L is $O(n + \ell^2)$. Hence Lang's Theorem can be solved for $c \in G_{\mathrm{ad}}(k_r)$ in time $O^\sim((n + \ell^2)^3 r^2 s^2 \log(q)^2)$, once we have a standard Chevalley basis for $E(k)$.

Using the isogeny map $G \to G_{\mathrm{ad}}$, we can apply Proposition 4.2(2) to obtain

Proposition 4.4. *Suppose that k has characteristic greater than 3. Let G be a k-split connected reductive group and let L be the Lie algebra of G. Let m be the exponent of the fundamental group of G. Let c be an element of $G(k_r)$ and suppose we are given s, the order of $c^{F^{r-1}} \cdots c^F c$. Let E be the variety of F-eigenvectors of c in L. We can find $a \in G(k_{rs})$ such that $c = a^{-F}a$ in Las Vegas time $O^\sim(n^6 m^2 r^2 s^2 \log(q)^2)$, plus the time needed to find a standard Chevalley basis of $E(k)$.*

We give an algorithm for finding a standard Chevalley basis in the next section. The timing of this algorithm is analysed in Section 6, leading to a proof of Theorem 1.2.

5. Computing a standard Chevalley basis

We now give an algorithm for constructing a Chevalley basis of the Lie algebra L of a k-split connected reductive group G. Recall that L is a p-Lie algebra [Jac62, Section V.7]. The first and hardest step is finding a k-split maximal toral p-subalgebra. This is similar to the algorithm of [dGIR96] for finding a Cartan subalgebra, but ensuring that the subalgebra is k-split makes things considerably more complex.

Our algorithm only works for fields of characteristic $p > 3$. Whenever possible we state results for characteristics 2 and 3, in the hope that the gaps in our argument for small p can be filled later.

We assume that L is given as a structure constant algebra, but we frequently compute in the adjoint representation. Throughout this section n denotes the reductive rank of G, ℓ denotes the semisimple rank of G, and d denotes the dimension of the Lie algebra L. Recall that our Steinberg presentation of G determines a k-split maximal torus T_0.

5.1. Toral subalgebras

A Lie algebra L over a field of characteristic p is called a *p-Lie algebra* if it is equipped with a map $p : L \to L$, written $x \mapsto x^p$, satisfying the axioms

$$(x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x, y), \tag{5}$$

$$(ax)^p = a^p x^p, \tag{6}$$

$$[x, y^p] = x(\mathrm{ad}\, y)^p, \tag{7}$$

where $x, y \in L$, $a \in \bar{k}$, s_i is defined in [Jac62, Section V.7], and a^p and $(\mathrm{ad}\, y)^p$ are the usual pth powers in $\bar{k}$ and the ring of linear maps on L, respectively.

Given values of the p-map on a basis of L, we can compute the values on an arbitrary element using Eqs. (5) and (6). But s_{p-1} involves Lie products of length p, so the time taken for this computation is not polynomial in $\log(p)$. For our purposes, it suffices to know the value of x^p up to the centre $Z(L)$. Given $x \in L$, we can use (7) to compute the coset $x^p + Z(L)$ in time $O^\sim(\ell^6 \log(p) \log(q))$, since $\dim(L/Z(L))$ is $O(\ell^2)$. We also define the *q-map* by applying the p-map e times, where $q = p^e$; values of this map modulo $Z(L)$ can be computed in time $O^\sim(\ell^6 \log(q)^2)$.

We say that $x \in L$ is *semisimple* if it is contained in the p-subalgebra generated by x^p. A *toral subalgebra* of L is a subalgebra defined over k consisting entirely of semisimple elements. Note that a toral subalgebra need not be a p-subalgebra. However every subalgebra H of L is contained in a minimal p-subalgebra called the *p-closure* of H in L. The p-closure of a toral subalgebra is toral, and so a maximal toral subalgebra is automatically a p-subalgebra. An n-dimensional toral p-subalgebra H is *k-split* if $H(k)$ is isomorphic, as a p-Lie algebra, to the vector space k^n with trivial Lie product and the p-map acting componentwise.

If L is the Lie algebra of a k-split connected reductive group G, then the values of the p-map on a Chevalley basis are

$$h_i{}^p = h_i \quad \text{and} \quad e_\alpha{}^p = 0,$$

provided that $p > 3$. Clearly $H_0 := L(T_0) = \langle h_1, \ldots, h_n \rangle$ is a k-split toral subalgebra.

We say that the Lie algebra L is *k-split* if it contains a maximal toral subalgebra which is k-split. The following theorem collects together the properties of toral subalgebras which we need.

Theorem 5.1. *Let L be the p-Lie algebra of a k-split connected reductive group G.*

(1) *L is k-split with split maximal toral subalgebra H_0.*
(2) *The centre of L is a k-split toral subalgebra when $p > 2$.*
(3) *Every toral subalgebra of L is abelian.*
(4) *Every (k-split) maximal toral subalgebra of L is the Lie algebra of a (k-split) maximal torus of G (when $p > 2$).*
(5) *The maximal toral subalgebras of L are G-conjugate.*
(6) *The k-split maximal toral subalgebras of L are $G(k)$-conjugate when $p > 2$.*

Proof. In Part (1) it only remains to prove maximality, which follows from [Hum67, Proposition 13.2]. Part (3) is given in [Hum78, Lemma 8.1] for characteristic zero, but the same proof works for positive characteristic. Part (5) is Corollary 13.5 of [Hum67].

We now prove Part (2). Let $\{e_\alpha, h_i\}$ be a Chevalley basis with respect to H_0. Suppose that $z \in Z(L)$ and write

$$z = \sum_{i=1}^{n} t_i h_i + \sum_{\alpha \in \Phi} a_\alpha e_\alpha.$$

Let $h_\alpha = \sum_{i=1}^n \langle e_i, \alpha^\star \rangle h_i$; then the coefficient of e_α in $[z, h_\alpha]$ is $2a_\alpha$. Since $[z, h_\alpha] = 0$ and $p > 2$, we get $a_\alpha = 0$. Hence z is in $H_0 = \langle h_1, \ldots, h_n \rangle$. Since H_0 is a split toral subalgebra, $Z(L)$ is also. (The idea for this proof is from [Hog82, Lemma 6.10].)

Every maximal toral subalgebra of L is the Lie algebra of a maximal torus of G by [Hum67, Proposition 13.2]. For $p > 2$, split tori correspond to split toral subalgebras by [Sel67, Theorem 9]. Hence Part (4) is proved.

```
MaximalToralSubalgebra := function(L)
  repeat take x random in L until x is semisimple
  let M = C_L(x)
  if M is abelian then
    return M
  else
    return MaximalToralSubalgebra(M)
  end if
end function
```

Algorithm 5. Finding a maximal toral subalgebra in L.

From now on we assume $p > 2$. By [Hum67, Proposition 13.6], $T \mapsto L(T)$ gives a one-to-one correspondence between maximal tori of G and maximal toral subalgebras of L. Once again, split tori correspond to split toral p-algebras. Part (6) now follows from the corresponding result for tori. □

Corollary 5.2. *Given a subalgebra H of L defined over k, we can determine if H is k-split maximal toral in time $O^{\sim}(n^3\ell^4 \log(q)^2)$.*

Proof. First check that H is abelian of dimension n. If so, then compute $Z(L)$ in time $O^{\sim}((n+\ell^2)^3 \log(q))$. Note that $H/Z(L)$ has dimension at most ℓ. By Theorem 5.1(2), it suffices to determine if $H/Z(L)$ is a split toral algebra. This is done by testing whether $b^q + Z(L) = b + Z(L)$ where $b + Z(L)$ runs over a basis of $L/Z(L)$. As we argued at the beginning of this section, this takes time $O^{\sim}(\ell^6 \log(q)^2)$ for each basis element. Using the fact that $\ell \leqslant n$, we get the result. □

Since semisimple elements are common in $L(k)$ (see Section 6) and the centraliser of such an element is reductive of rank n, we can find a maximal toral subalgebra by Algorithm 5.

The basic idea of our method is to randomly select a series of increasingly split maximal toral subalgebras. We now assign a conjugacy class of W to every maximal toral subalgebra H, which measures how split H is. See [Leh92] for a more detailed version of this construction. We will denote the adjoint action of G on L by exponentiation. By Theorem 5.1(5) there exists $g \in G(\bar{k})$ such that $H = H_0{}^g$. Note that $H_0{}^F = H_0$ and $H^F = H$, since both are defined over k. Now

$$H_0{}^{g^F g^{-1}} = \left(\left(H_0{}^g\right)^F\right)^{g^{-1}} = \left(H^F\right)^{g^{-1}} = H^{g^{-1}} = H_0,$$

so $g^F g^{-1}$ is in $N_G(H_0) = N_G(T_0)$. Let w be the image of $g^F g^{-1}$ under projection onto the Weyl group $W = N_G(T_0)/T_0$. The element w is uniquely determined by H up to conjugacy in W.

5.2. Root decompositions of L

The *root decomposition* of L with respect to H_0 is

$$L = H_0 \oplus \bigoplus_{\alpha \in \Phi_k} L_\alpha,$$

where the *root space* $L_\alpha = \{b \in L \mid [b,h] = \alpha(h)b \text{ for all } h \in H_0\}$ and each root $\alpha \in \Phi_k = \Phi(L, H_0)$ is a linear functional $H_0 \to \bar{k}$. This decomposition is defined over k by [Sel67, Theorem 6]. When the characteristic p of k is greater than 3 or $p = 3$ and G has no components of type G_2 and A_2, [Hog82] ensures that each space L_α has dimension one. In this case there is a bijective correspondence between Φ_k and Φ, the root system contained in R.

Let H be a maximal toral subalgebra of L, fix $g \in G(\bar{k})$ such that $H = H_0{}^g$ and let w be the image of $g^F g^{-1}$ in W. For $\alpha \in \Phi_k$, define $\alpha^g : H \to \bar{k}$ by $\alpha^g(h) = \alpha(h^{g^{-1}})$. As $p > 2$, each $\alpha \in \Phi_k$ induces a nonzero map α^g and so the root space decomposition with respect to H is a direct sum

```
GeneralisedRoots := function(L, H)
  let h_1, ..., h_n be a basis of H
  let F = {()} and define L_() = L
  for i = 1, ..., n do
    let F' = ∅
    for f ∈ F do
      compute g, the characteristic polynomial of h_i on L_f
      for f_i an irreducible factor of g do
        add (f_1, ..., f_{i-1}, f_i) to F' where f = (f_1, ..., f_{i-1})
        define L_(f_1,...,f_i) = {x ∈ L_f | x f_i(ad(h_i)) = 0}
      end for
    end for
    let F = F'
  end for
  remove (X, ..., X) from F        [since L_(X,...,X) = H]
  return F
end function
```

Algorithm 6. Generalised roots.

$$L = H \oplus \bigoplus_{\alpha \in \Phi_k} L_{\alpha^g},$$

where $L_{\alpha^g} = \{b \in L \mid [b,h] = \alpha^g(h)b \text{ for all } h \in H\} = L_{\alpha}{}^g$. This decomposition is not defined over k in general, but certainly over $\bar{k}$. It has $|\Phi_k|$ components distinct from H.

Fix a basis $h_1, \dots, h_n$ of H and let $f = (f_1, \dots, f_n)$ be a sequence of irreducible polynomials in $k[X]$ with $f_i(X) \neq X$ for at least one i. Define

$$L_f = \big\{ y \in L \;\big|\; y f_i\big(\mathrm{ad}(h_i)\big) = 0 \text{ for } i = 1, \dots, \ell \big\}. \tag{8}$$

If $L_f \neq 0$, we call f a *generalised root* and L_f a *generalised root space*. The *generalised root decomposition* of L with respect to H is

$$L = H \oplus \bigoplus_{f \in \mathcal{F}} L_f, \tag{9}$$

where $\mathcal{F} = \mathcal{F}(L,H)$ is the set of generalised roots of L with respect to H. This decomposition is defined over k. The generalised roots are computed by Algorithm 6. Complete factorisation of a polynomial of degree d over k takes Las Vegas time $O^{\sim}(d^2 \log(q)^2)$ by [vzGS92]. Computing the nullspaces $L_{(f_1,\dots,f_i)}$ is the dominant contribution to the running time of this algorithm. Since the sum of the degrees of all the f_i is at most nd, the algorithm takes time $O^{\sim}(nd^3 \log(q)^2)$.

In fact, we do not apply this algorithm directly to L, since we want our time to depend on ℓ but not on n. Rather, we apply it to the quotient of L by a Lie algebra of its centre. This is necessary for analysing the recursion in Algorithm 8.

Given a generalised root $f \in \mathcal{F}(L,H)$, the subspace L_f is a direct sum of components L_{α^g} of the root decomposition with respect to H. So we can partition Φ into subsets Φ_f such that $L_f = \bigoplus_{\alpha \in \Phi_f} L_{\alpha^g}$. Define the *degree* of f to be the lowest common multiple of the degrees of the f_i. Given a generalised root f, we define

$$f_- = \big((-1)^{\deg(f_1)} f_1(-X), \dots, (-1)^{\deg(f_n)} f_n(-X)\big).$$

Clearly $\Phi_{f_-} = -\Phi_f$. Note that we can have $f = f_-$ when the degree of f is greater than one.

We now prove some properties of the sets Φ_f.

Lemma 5.3. *Suppose $|\Phi| = |\Phi_k|$ (so $p > 3$ or $p = 3$ and the type of G is distinct from G_2 and A_2). Let f be a generalised root of $L = L(G)$ with respect to H.*

(1) *The action of F on $\{L_{\alpha^g} \mid \alpha \in \Phi_f\}$ is equivalent to the action of w on Φ_f.*
(2) *Φ_f is a union of orbits of w on Φ.*
(3) *If $\deg(f) = 1$, then w acts trivially on Φ_f. If in addition $q > 3$, then Φ_f contains a single root.*
(4) *Suppose $p > 2$. If $\deg(f) = 2$ and $f = f_-$, then w acts on Φ_f by negation.*

Proof. Write $g^F g^{-1} = t\dot{w}$ for some $t \in T_0$. Now

$$L_{\alpha^g}{}^F = L_{\alpha}{}^{gF} = L_{\alpha}{}^{F^{-1}gF} = L_{\alpha}{}^{g^F} = L_{\alpha}{}^{t\dot{w}g} = L_{\alpha w}{}^g = L_{(\alpha w)^g},$$

and so Part (1) is proved. Part (2) follows since $L_f{}^F = L_f$.

Part (3) holds because L_f is a root space when $\deg(f) = 1$.

Suppose $\deg(f) = 2$ and $f = f_-$. Let $\alpha \in \Phi_f$. Then $L_{\alpha^g}{}^F = L_{(\alpha w)^g}$ and so $(\alpha w)^g(h_i)$ and $\alpha^g(h_i)$ are conjugate roots of f_i. But if $\deg(f_i) = 2$, then $f = f_-$ implies that the conjugate roots are negatives of each other. And if $\deg(f_i) = 1$, then $f = f_-$ implies that the only root of f_i is zero. In either case $(\alpha w)^g(h_i) = -\alpha^g(h_i)$ and so w acts on Φ_f by negation. □

5.3. Fundamental subalgebras

Now that we have the generalised root decomposition of L with respect to H, we consider the subalgebra generated by a generalised root space L_f. Such subalgebras often turn out to be fundamental in the following sense.

We define a (*split*) *fundamental subgroup* of G as a connected reductive subgroup normalised by a (split) maximal torus. A subalgebra M of L is (*split*) *fundamental* if it is normalised by a (split) maximal toral subalgebra of L.

Lemma 5.4. *Let Ψ be a closed subsystem of Φ and H a maximal toral subalgebra of L. Then there is a fundamental Lie subalgebra of L with root system Ψ normalised by H.*

Proof. There exists $g \in L$ such that $H = H_0 g$. Put $M = H + \sum_{\alpha \in \Psi} L_{\alpha^g}$. Then M is a subalgebra of L normalised by H. □

The most important properties of such algebras for our purposes are

Theorem 5.5. *Suppose $p > 2$. Let M be a subalgebra of L normalised by the maximal toral subalgebra H.*

(1) *$M \cap H$ is a maximal toral subalgebra of M.*
(2) *The subspace $H + M$ of L is the Lie algebra of a closed connected algebraic subgroup G_M of G.*

Proof. We have $H \leqslant C_{M+H}(H) \leqslant C_L(H) = H$, so $M + H$ has root decomposition

$$M + H = H \oplus \bigoplus_{\beta} M_\beta, \tag{10}$$

where β runs over $\Phi(M + H, H)$, the set of roots of $M + H$ with respect to H. Suppose $m + h \in M_\beta$ where $m \in M$ and $h \in H$. Then, for all $h' \in H$, $[m, h'] = [m + h, h'] = \alpha(h')(m + h)$. But $[m, h'] \in M$, and so $h \in M$ and $M_\beta \leqslant M$. So, by intersecting (10) with M, we obtain the root decomposition

$$M = (H \cap M) \oplus \bigoplus_{\beta} M_\beta,$$

and so $H \cap M$ is a maximal toral subalgebra of M and (1) is proved.

As for (2), H normalises M, so the subspace $H+M$ is a Lie subalgebra of L. By Theorem 5.1(4), there is maximal torus T of G whose Lie algebra coincides with H. For each $\beta \in \Phi(M+H,H)$ as above, there is a root group T_β in G with respect to T whose Lie algebra is M_β. The product of all T_β for $\beta \in \Phi(M+H,H)$ and T is a closed connected algebraic subgroup of G with Lie algebra $M+H$. This settles the theorem. □

Recall that the closure $\overline{\Psi}$ of $\Psi \subseteq \Phi$ is just the set of all roots that can be written as a sum of elements of Ψ. Note that if $\overline{\Psi}$ is also closed under negation, it is a subsystem. If $\overline{\Psi}$ is a subsystem, we say $w \in W$ is *inner* on $\overline{\Psi}$ if the action of w on $\overline{\Psi}$ is induced by an element of $W(\overline{\Psi})$.

Lemma 5.6. *Suppose $|\Phi| = |\Phi_k|$. Let M be the subalgebra generated by $\sum_{\alpha\in\Psi} L_{\alpha^g}$, where Ψ is a w-invariant subset of Φ.*

(1) *If Ψ is a single w-orbit, then either $\overline{\Psi}$ is a subsystem of Φ or M is soluble.*
(2) *If $\overline{\Psi}$ is a subsystem and w is inner on $\overline{\Psi}$, then M is split fundamental.*

Proof. Since $[\sum_{\alpha\in\Psi} L_{\alpha^g}, H] \leqslant \sum_{\alpha\in\Psi} L_{\alpha^g}$, we have $[M,H] \leqslant M$ and so M is normalised by H. Since $[L_\alpha, L_\beta] \leqslant L_{\alpha+\beta}$ (recalling that $L_0 = H$), we have

$$M = (H\cap M) \oplus \bigoplus_{\alpha\in\overline{\Psi}} L_{\alpha^g}.$$

Let $\Psi = \Psi_1 \cup \cdots \cup \Psi_m$ be the finest decomposition of Ψ into pairwise orthogonal subsets. Then $\overline{\Psi} = \overline{\Psi}_1 \cup \cdots \cup \overline{\Psi}_m$ is also an orthogonal decomposition. Clearly w permutes the sets Ψ_i and, since w is transitive on Ψ, it must be transitive on them. Since $-\overline{\Psi}_1$ is never orthogonal to $\overline{\Psi}_1$, we either have $-\overline{\Psi}_1 = \overline{\Psi}_1$ or $-\overline{\Psi}_1$ is disjoint from $\overline{\Psi}_1$. By the transitivity of w, whichever of these cases holds for $-\overline{\Psi}_1$, also holds for all $-\overline{\Psi}_i$. In particular, $\overline{\Psi}$ is closed under negation iff $\overline{\Psi}_1$ is. Let ψ be the sum of all the elements of $\overline{\Psi}_1$. Now $\overline{\Psi}_1$ is closed under negation iff $\psi = 0$ (since $\psi = 0$ implies $-\alpha = \sum_{\beta\in\overline{\Psi}_1,\,\beta\neq\alpha} \beta \in \overline{\Psi}_1$ for all $\alpha \in \overline{\Psi}_1$, and the converse is trivial). We define $M_i = H_i \oplus \bigoplus_{\alpha\in\overline{\Psi}_i} L_{\alpha^g}$, where H_i is the subalgebra of H generated by $[L_{\alpha^g}, L_{-\alpha^g}]$ for all $\alpha \in \overline{\Psi}_i$. Note that $M = \sum_i M_i$. Suppose first that $\psi \neq 0$. Then the root subsystem generated by Ψ_1 is just $\overline{\Psi}_1 \cup -\overline{\Psi}_1$. Since this root subsystem is irreducible, ψ induces an ordering on it which makes $\overline{\Psi}_1$ the set of positive roots. Hence M_1 is contained in the Borel subalgebra of the Lie algebra of a simple group, and so must be soluble. The transitivity of w on the sets $\overline{\Psi}_i$ implies that M_i is soluble for every i, and so $M = \bigoplus_i M_i$ is soluble. If $\psi = 0$, then $\overline{\Psi}_1$ is an irreducible root subsystem and so Ψ is a root subsystem of Φ. Part (1) is now proved.

Now suppose that $\overline{\Psi}$ is closed under negation and w is inner on $\overline{\Psi}$. By Lang's Theorem applied to $M+H$, cf. Theorem 5.5(2), we can find $h \in G_M$ such that $h^F h^{-1} = \dot{w}$. On the other hand, g satisfies $g^F g^{-1} = t\dot{w}$ for some $t \in T_0$. Now the map $\dot{w}F$ is a nonstandard Frobenius endomorphism since $\dot{w}^F = \dot{w}$ and so $(\dot{w}F)^m = F^m$, where m is the order of $\dot{w}$. Furthermore ${T_0}^{\dot{w}F} = T_0$. So, by Lang's Theorem in T_0, there is a $u \in T_0$ such that $t = u^{\dot{w}F} u^{-1}$. Set $\tilde{g} = u^{-\dot{w}} g$, so that

$$\tilde{g}^F \tilde{g}^{-1} = u^{-\dot{w}F} g^F g^{-1} u^{\dot{w}} = u^{-\dot{w}F} t u \dot{w} = \dot{w}$$

and ${H_0}^{\tilde{g}} = {H_0}^{\dot{w}^{-1}u^{-1}\dot{w}g} = {H_0}^g = H$. Hence $h^F h^{-1} = \tilde{g}^F \tilde{g}^{-1}$, that is $\tilde{g}h^{-1}$ is defined over k and so $H^{h^{-1}} = {H_0}^{\tilde{g}h^{-1}}$ is split. So

$$\left[M, H^{h^{-1}}\right] = \left[M^h, H\right]^{h^{-1}} = [M,H]^{h^{-1}} \leqslant M^{h^{-1}} = M,$$

which shows that M is split fundamental. □

```
SplitMaximalToralSubalgebraA1 := function(L)        [L of type A1]
  repeat take x random in L
  until the minimal polynomial of ad(x) factors into distinct linear terms
  return C_L(x)
end function
```

Algorithm 7. Finding a split maximal toral subalgebra in L of type A_1.

We will apply the lemma to the Lie subalgebra of L generated by L_f; here $\Psi = \Phi_f$ as defined in (8). It is w-invariant according to Lemma 5.3(2).

5.4. Finding a split maximal toral subalgebra

We begin with the smallest simple Lie algebras known: those of type A_1, that is, isogenous to $\mathfrak{sl}_2$. As p is odd, there is in fact only one isomorphism class of such Lie algebras for each k. An advantage of this type is that each involution induced on a subroot system of this type is inner, so Lemma 5.6(2) applies. We indicate how to find a split maximal toral subalgebra in such an algebra and provide a timing analysis. The timings for the general case will be dealt with in Section 6.4.

Lemma 5.7. *Let M be a Lie algebra of type A_1 and reductive rank 1 over k, with $q = |k|$ odd, $q \geqslant 5$. Then there are $q^3 - q^2$ nonzero semisimple elements in M. Of these, exactly $\frac{1}{2}(q^3 - q)$ have a characteristic polynomial that factorises completely into linear terms. In particular, we can find a split maximal toral subalgebra of M in Las Vegas time $O^\sim(\log(q)^2)$.*

Proof. As the characteristic of k is distinct from 2, each Lie algebra of type A_1 and reductive rank 1 over k is isomorphic to the standard Lie algebra of A_1 over k. Therefore, without loss of generality, we may assume that M is the Lie algebra of 2×2 matrices over k having trace 0. In this model the counts for semisimple elements are easily verified.

Algorithm 7 gives an explicit description of a Las Vegas algorithm for finding a split maximal toral subalgebra of M. It uses the characterisation of semisimple elements as those whose minimal polynomial is squarefree. As the minimal polynomial of $\mathrm{ad}(x)$ for $x \in M$ has degree at most 3 with one factor equal to X, the hardest part of the factorisation can be reduced to finding the square root of an element in k. Hence, computations can be carried out in time $O^\sim(\log(q)^2)$.

According to the count of split semisimple elements above, by a single choice of $x \in M$ in Algorithm 7 we obtain a split maximal toral subalgebra of M with probability at least

$$\frac{q^3 - q}{2q^3} = \frac{1}{2}\left(1 - \frac{1}{q^2}\right) \geqslant \frac{12}{25}.$$

This shows that the Las Vegas time is also $O^\sim(\log(q)^2)$. □

The probability estimate in the above proof is a special case of the lower bound in Proposition 6.1 below.

Suppose now that we have found a nontrivial split fundamental subalgebra M of type A_1. The following proposition shows that we can use recursion to find a split maximal toral subalgebra of L.

Proposition 5.8. *Suppose $p > 2$. Let M be a split fundamental subalgebra of L of type A_1. Let K be a split maximal toral subalgebra of M. Then $C_L(K)$ is a split fundamental subalgebra of L. Moreover, it is the Lie algebra of the k-split closed reductive subgroup $C_G(K)$ of G of reductive rank n.*

Proof. Let H be a split maximal toral subalgebra of L that normalises M. Let G_M be the split fundamental subgroup of G defined in Theorem 5.5(2). By construction, the maximal torus T corresponding to H (cf. Theorem 5.1(4)) normalises G_M and so H normalises M. Moreover, by Theorem 5.5(1), $H \cap M$ is a split maximal toral subalgebra of M. By Theorem 5.1(6), there is a conjugator g' in $G_M(K)$ so that

```
SplitMaximalToralSubalgebra := function(L, Z)        [Z ⩽ Z(L)]
  repeat
    let H/Z = MaximalToralSubalgebra(L/Z)
    if H is split then return H end if
    let F = GeneralisedRoots(L/Z, H/Z)
    if there exists f ∈ F with deg(f) = 1 then
      let M/Z = ⟨(L/Z)_f + (L/Z)_{f_-}⟩
      let K/Z = H/Z ∩ M/Z
      return SplitMaximalToralSubalgebra(C_L(K), K)
    elif there exists f ∈ F with deg(f) = 2 and f = f_- then
      let M/Z = ⟨(L/Z)_f⟩
      let K/Z = SplitMaximalToralSubalgebraA1(M/Z)
      return SplitMaximalToralSubalgebra(C_L(K), K)
    end if
  until L = Z
  return Z
end function
```

Algorithm 8. Finding a split maximal toral subalgebra.

$K = (H \cap M)^{g'} = H^{g'} \cap M$. But then $H^{g'}$ is a split maximal toral subalgebra of L containing K. As $H^{g'}$ is abelian, it follows that $H^{g'}$ is a split maximal toral subalgebra of L contained in $C_L(K)$.

By [Hum75, Corollary 26.2A], $C_G(K)$ is a reductive group. It is normalised by $T^{g'}$ and so it is k-split fundamental. Also, $L(C_G(K)) = C_L(K)$ by [Spr98, Theorem 4.4.4]. □

We now have a method for finding split maximal toral subalgebras of L, as documented in Algorithm 8. Let $p > 3$.

For the sake of efficiency, we take $Z = Z(L)$ initially (the algorithm can also be invoked with $Z = \{0\}$). Let us argue why. By Theorem 5.1(2), the centre $Z(L)$ of L is contained in H. Moreover, by (9), there is a basis $h_1, \ldots, h_n$ for $H(k)$ such that, for some $r \leqslant n$, $Z = \langle h_1, \ldots, h_r \rangle$ is central. Extend this to a basis of $L(k)$. Let ϕ be the pullback map $L/Z \to L$ via this basis. We compute in L/Z, since it has dimension $O(\ell^2)$ independent of n, and the results are then transfered into L via ϕ. Let $\mathcal{F}$ be the set of generalised roots of $L/Z(L)$ with respect to $H/Z(L)$. Given $f = (f_1, \ldots, f_m) \in \mathcal{F}$ define the sequence $f' = (X, \ldots, X, f_1, \ldots, f_m)$ of length n. It is now easy to see that $\phi((L/Z)_f) = L_{f'}$. Hence the generalised root space decomposition of L with respect to H follows immediately once we have the decomposition of L/Z with respect to H/Z. Since the dimension of L/Z is $O(\ell^2)$, the generalised root space decomposition of L/Z can be computed in time $O^{\sim}(\ell^7 \log(q)^2)$.

Working modulo Z, Algorithm 8 finds a maximal toral subalgebra H of L by use of Algorithm 5. If it is split, we are done. Otherwise, we continue by computing its generalised roots $\mathcal{F}$.

Assume $\deg(f) \leqslant 1$ or $\deg(f) = 2$ and $f = f_-$ for some $f \in \mathcal{F}$. Then $M_f(k) = \langle L_f(k) + L_{f_-}(k) \rangle$ is a subalgebra of type A_1 normalised by H. For $\deg(f) = 1$, this is immediate from Lemma 5.3(3), so, in order to see this, assume $\deg(f) = 2$ and $f = f_-$. If i is such that $\deg(f_i) = 2$, then $f_i = X^2 - a_i$ for some $a_i \in k$, and so f_i factors into linear terms over k_2, whereas $f_i = X$ if $\deg(f_i) = 1$; therefore, $M_f(k_2)$ is generated by $L_f(k_2) = L_\chi(k_2) + L_{-\chi}(k_2)$ for some linear form χ on $H(k_2)$ (with both L_χ and $L_{-\chi}$ of dimension 1 as $p > 3$); as w interchanges L_χ and $L_{-\chi}$, it is inner on $\{\chi, -\chi\}$ and so Lemma 5.6(2) shows that the Lie algebra $M_f(k)$ is of type A_1.

We continue with $f \in \mathcal{F}$ as above. A pair of linearly independent nilpotent elements in M_f can be transformed, by an element of $G(k)$, to a pair of elements $e_\alpha, e_{-\alpha}$ of the standard Chevalley basis for some $\alpha \in \Phi$. Hence, there is an element $g' \in G(k)$ so that $M_f = \langle e_\alpha, e_{-\alpha} \rangle^{g'}$. Now M_f is normalised by the split maximal toral subalgebra $H^{g'}$ of L, so it is a split fundamental subalgebra of L. If $\deg(f) = 1$, then $K = H \cap M$ is a split maximal toral subalgebra of M; if $\deg(f) = 2$ and $f = f_-$, a split maximal toral subalgebra K of M is found by Algorithm 7.

By Proposition 5.8, a split maximal toral subalgebra of the Lie algebra $C_L(K)$ of the reductive group $C_G(K)$ has rank n and so is also a split maximal toral subalgebra of L. Since K is contained in the centre of $C_L(K)$, the recursion with $(C_L(K), K)$ instead of (L, Z) is valid. At each recursive call, the rank of Z has increased, so the total number is at most ℓ if we start with $Z = Z(L)$ and n if we start with $Z = \{0\}$.

```
StandardChevalleyBasis := function(G, L)
  let H = SplitMaximalToralSubalgebra(L, Z(L))
  compute the root system Φ_k = Φ(L, H) and root spaces L_α for α ∈ Φ_k
  find simple roots α_1, ..., α_ℓ of Φ_k and identify them with the simple roots of Φ
  for i = 1, ..., ℓ do
    let α = α_i
    choose nonzero e_α ∈ L_α and f_α ∈ L_{-α}
    find a ∈ k such that [e_α, [f_α, e_α]] = 2a e_α
    let e_{-α} = f_α / a
  end for
  for γ a nonsimple root do
    let (α, β) be the extraspecial pair of γ
    let e_γ = [e_α, e_β]/N_{αβ}, e_{-γ} = [e_{-α}, e_{-β}]/N_{-α,-β}
  end for
  let h_1, ..., h_n be a solution of (2) and (3)
  return h_i for i ∈ {1, ..., n} and e_α for α ∈ Φ
end function
```

Algorithm 9. Finding a standard Chevalley basis.

In Section 6, we give a time analysis of Algorithm 8.

5.5. Finding a standard Chevalley basis

We now show how to find a standard Chevalley basis for $L(k)$, as defined in Section 4.3. We assume that we are given a root datum (X, Φ, Y, Φ^*) for the split connected reductive group G with Lie algebra L. Our computations use the root datum, but not the group.

Let H be a k-split maximal toral subalgebra of L computed as in Section 5.4. The root decomposition

$$L = H \oplus \bigoplus_{\alpha \in \Phi_k} L_\alpha$$

can be computed by linear algebra over k. The identification of Φ_k with Φ can be found by computing simple roots for each system and reordering the roots so that the Cartan matrices are identical. The details are given in [dG00, Chapter 5] for characteristic zero, but the method is identical in our case.

Fix dual bases $e_1, \ldots, e_n$ for X and $f_1, \ldots, f_n$ for Y. Let $\alpha_1, \ldots, \alpha_\ell$ be simple roots of Φ. Then Algorithm 9 can be used to find elements e_α in each L_α satisfying (4) of Section 4.3. We take the $N_{\alpha\beta}$ as in a *standard* Chevalley basis (Section 4.3). So, for each extraspecial pair (α, β), we have $0 < N_{\alpha\beta} \leqslant 3$ and hence division by $N_{\alpha\beta}$ is not a problem.

Finding a basis $h_1, \ldots, h_n$ of $H(k)$ satisfying Eqs. (2) and (3) is just a matter of solving linear equations in n^2 variables. We conclude

Lemma 5.9. *Algorithm* 9 *finds a standard Chevalley basis in time* $O^\sim(n^6 \log(q)^2)$ *plus the time to compute the split maximal toral subalgebra* H.

6. Reflection derangements and time analysis

Let L be the Lie algebra of the k-split connected reductive linear algebraic group G. We now find bounds on the probability of finding a maximal toral subalgebra $H \leqslant L$ and a set A of generalised roots such that M_A is known to be split fundamental. To simplify our analysis, we just bound the probability that Algorithm 5 finds a maximal toral subalgebra in a single step, or equivalently that the random element chosen is regular semisimple. Section 6.1 gives bounds on the frequencies of regular semisimple elements corresponding to Weyl group elements. In Section 6.2, we bound the proportion of suitable Weyl group elements. We give the proof of Theorem 1.2 in Section 6.4.

Throughout this section, n is the reductive rank of G, ℓ is the semisimple rank of G, d is the dimension of L, and $d_1, \ldots, d_\ell$ are the invariant degrees of G as defined in [Car72, Section 9.3].

6.1. Regular semisimple elements

An element of L is *regular semisimple* if its centraliser is a maximal toral subalgebra. For any subvariety S of L, let S_{rss} be the variety of regular semisimple elements in S. Recall from Section 5.1 that the maximal toral subalgebras of L are classified up to $G(k)$-conjugacy by the conjugacy classes of W. Fix w in W and let $L_{\mathrm{rss},w}$ be the set of elements $x \in L$ which are regular semisimple and such that there exists $g \in G$ with $C_L(x) = H_0{}^g$ and $g^F g^{-1} \in T_0 \dot{w}$. Although we give direct proofs, many results in this section also follow from Gus Lehrer's analysis of hyperplane complements [Leh92,Leh98].

The following result bounds our chances of finding a regular semisimple element in $L(k)$ whose centraliser corresponds to the W-class of a given w.

Proposition 6.1. *Let L be the Lie algebra of a k-split connected reductive group G with root datum $(X, \Phi, Y, \Phi^\star)$. Let w be an element of the Weyl group W. Define*

$$Q_w(x) = \frac{\prod_{i=1}^{\ell}(1 - x^{d_i})}{\det_Y(1 - wx)} \in \mathbb{Q}(x).$$

Then

$$\left(1 - \sum_{i=1}^{\ell} \frac{c_i}{q^i}\right) Q_w(1/q) \frac{|w^W|}{|W|} \leqslant \frac{|L_{\mathrm{rss},w}(k)|}{|L(k)|} \leqslant Q_w(1/q) \frac{|w^W|}{|W|},$$

where $c_i = c_i(w)$ is the number of w-orbits in Φ consisting of roots α with the property that i is the largest integer for which $\alpha, \alpha w, \ldots, \alpha w^{i-1}$ are $\bar{k}$-linearly independent.

Proof. Fix some $g \in G$ such that $g^F g^{-1} = \dot{w}$ and define $H_w = H_0{}^g$. Let $T_w = T_0{}^g$ so that $L(T_w) = H_w$. Then

$$L_{\mathrm{rss},w}(k) = \left\{x \in L_{\mathrm{rss}}(k) \;\middle|\; x \in H_w(k)^h \text{ for some } h \in G(k)\right\},$$

which is in one-to-one correspondence with

$$\left\{(x, H) \in L_{\mathrm{rss}}(k) \times H_w(k)^{G(k)} \;\middle|\; x \in H\right\}.$$

Since $N_{G(k)}(H_w(k))/T_w(k) \cong C_W(w)$, we have $|H_w(k)^{G(k)}| = \frac{|G(k)|}{|T_w(k)||C_W(w)|}$. Hence

$$\frac{|L_{\mathrm{rss},w}(k)|}{|L(k)|} = \left|(H_w)_{\mathrm{rss}}(k)\right| \frac{|G(k)|}{|L(k)||T_w(k)|} \frac{|w^W|}{|W|}.$$

Given a root $\alpha \in \Phi$, define

$$H_\alpha = \left\{h \in H_w \;\middle|\; \alpha^g(h) = 0\right\}.$$

Then H_α is a hyperplane in H_w and $(H_w)_{\mathrm{rss}} = H_w - \bigcup_{\alpha \in \Phi} H_\alpha$. Now ${H_\alpha}^F = H_{\alpha w}$, so $H_\alpha(k) = (\bigcap_j H_{\alpha w^j})(k)$. This space has codimension i, the largest integer such that $\alpha, \alpha w, \ldots, \alpha w^{i-1}$ are linearly independent. So, for each $i = 1, \ldots, \ell$, we are removing c_i subspaces of codimension i from a k-space of dimension n. Hence

$$q^n \left(1 - \sum_{i=1}^{\ell} \frac{c_i}{q^i}\right) \leqslant \left|(H_w)_{\mathrm{rss}}(k)\right| \leqslant q^n.$$

Using Theorem 9.4.10 of [Car72] and the fact that our group is untwisted, we get

$$\left|G(k)\right| = q^d \prod_{i=1}^{\ell} \left(1 - \frac{1}{q^{d_i}}\right).$$

Using Proposition 3.3.5 of [Car93] and the fact that F is the standard Frobenius, we find that $T_w(k)$ has order $\det_Y(qI - w)$. Hence

$$\frac{|G(k)|}{|L(k)||T_w(k)|} = \frac{q^d \prod_i (1 - 1/q^{d_i})}{q^d \det_Y(qI - w)} = \frac{Q_w(1/q)}{q^n}. \qquad \square$$

6.2. Reflection derangements

Recall from Section 5.2 that there is a relationship between the generalised roots f with respect to a maximal toral subalgebra and the orbits of the corresponding Weyl group element w on Φ. This relationship need not be a one-to-one correspondence. As we saw in Lemma 5.3(3) and (4), this relationship is almost a one-to-one correspondence when the degree of f is one, or the degree is two and $f = f_-$. This happens when there is a root α such that $\alpha w = \pm\alpha$. In other words, when a reflection s_α is fixed under conjugation by w.

In this section, we count the number of Weyl group elements of this kind. Given a permutation representation of a group, an element of the group is called a *derangement* with respect to the representation if it fixes no points at all. The proportion of derangements of the symmetric group Sym_t acting on t letters is known to approach $1/e$ as $t \to \infty$. We give similar results for a Weyl group acting on its reflections by conjugation. We refer to these elements as *reflection derangements*. We are grateful to Anthony Henderson for helping us with the proof of this proposition.

Proposition 6.2. *If W is an irreducible Coxeter group of classical type A_ℓ, $\mathrm{B}_\ell/\mathrm{C}_\ell$, or D_ℓ, then the proportion of its reflection derangements approaches $2e^{-3/2}$, $e^{-5/4}$, or $2e^{-5/4} + (4e)^{-1}$, respectively, as $\ell \to \infty$. For exceptional types, the proportions are as listed below*:

G_2	F_4	E_6	E_7	E_8
1/3	1/4	1409/2592	1646/2835	3385549/6220800

Proof. Denote by f the number of reflection derangements of W. We wish to determine $f/|W|$.

Type A_ℓ: The Weyl group $W(\mathrm{A}_\ell)$ can be identified with the symmetric group $\mathrm{Sym}_{\ell+1}$ on $\ell + 1$ letters. Write $m = \ell + 1$ and write d_m for the proportion of permutations in Sym_m without fixed points in $\{1, \ldots, m\}$. Denote by R_m the set of all permutations in Sym_m with at most one fixed point in $\{1, \ldots, m\}$.

An element of Sym_m does not fix a reflection if, and only if, it belongs to R_m and does not contain a transposition (i, j) in its cycle decomposition. So

$$f = \left| R_m - \bigcup_{1 \leqslant i < j \leqslant m} R_m^{i,j} \right|,$$

where

$$R_m^{ij} = \left\{ w \in R_m \;\middle|\; w \text{ contains } (i, j) \right\}.$$

We compute f by inclusion/exclusion. As R_m^{ij} and $R_m^{ij'}$ intersect trivially for $j \neq j'$ we can find f as an alternating sum over h-tuples of commuting transpositions:

$$\sum_{h=0}^{\lfloor m/2 \rfloor} (-1)^h \binom{m}{2h} \frac{(2h)!}{2^h h!} |R_{m-2h}|.$$

Since, clearly, $|R_m| = d_m + m d_{m-1}/m$,

$$f = m! \sum_{h=0}^{\lfloor m/2 \rfloor} \left(-\frac{1}{2}\right)^h \frac{1}{h!} (d_{m-2h} + d_{m-2h-1}).$$

As $\lim_{m\to\infty} d_m = 1/e$, the required proportion tends to

$$\lim_{m\to\infty} \frac{f}{m!} = \sum_{h=0}^{\infty} \left(-\frac{1}{2}\right)^h \frac{1}{h!} \frac{2}{e} = e^{-\frac{1}{2}} \frac{2}{e} = 2e^{-\frac{3}{2}}.$$

Types B_ℓ *and* C_ℓ: The Weyl group $W = W(\mathrm{B}_\ell) = W(\mathrm{C}_\ell)$ can be identified with the group of all permutations w of $\{\pm 1, \ldots, \pm \ell\}$ such that $(-i)w = -(iw)$. Define the homomorphism $\phi : W \to \mathrm{Sym}_\ell$ by $iw^\phi = |iw|$. Then $w \in W$ fixes no reflections if, and only if, w^ϕ is a derangement of Sym_ℓ and, for every transposition (i, j) contained in the cycle decomposition of w^ϕ, either $(i, j, -i, -j)$ or $(j, i, -j, -i)$ is contained in the cycle decomposition of w.

Writing S_ℓ for elements of W such that w^ϕ is a derangement and

$$S_\ell^{ij} = \left\{ w \in S_\ell \;\middle|\; w \text{ contains } (i, j)(-i, -j) \text{ or } (i, -j)(-i, j) \right\},$$

we find that

$$f = \left| S_\ell - \bigcup_{1 \leqslant i < j \leqslant \ell} S_\ell^{ij} \right|.$$

Again, we can count f by taking alternating sums over h-tuples of commuting transpositions in W^ϕ. As each transposition in the decomposition of an element of w^ϕ corresponds to two 4-cycles as indicated above, we find an extra factor 2^h compared to the A_ℓ case:

$$\sum_{h \geqslant 0,\, 2h \leqslant \ell} (-1)^h \binom{\ell}{2h} \frac{(2h)!}{2^h h!} 2^h |S_{\ell-2h}|.$$

As $|S_\ell| = 2^\ell \ell! d_\ell$,

$$f = \sum_{h \geqslant 0,\, 2h \leqslant \ell} (-1)^h \frac{\ell!}{h!} 2^{\ell-2h} d_{\ell-2h}.$$

As $\lim_{m\to\infty} d_m = 1/e$ and $|W(\mathrm{B}_\ell)| = 2^\ell \ell!$, the required proportion tends to

$$\lim_{m\to\infty} \frac{f}{2^\ell \ell!} = \sum_{h=0}^{\infty} \left(-\frac{1}{4}\right)^h \frac{1}{h!} \frac{1}{e} = e^{-\frac{1}{4}} e^{-1} = e^{-\frac{5}{4}}.$$

Type D_ℓ: The Weyl group $W(\mathrm{D}_\ell)$ is the subgroup of $W(\mathrm{B}_\ell)$ consisting of all elements w such that $\prod_{i=1}^{\ell} iw$ is positive. In cycle notation, this means that w has an even number of negative cycles (that is, cycles in which both positive and negative numbers occur).

Define $\phi : W \to \mathrm{Sym}_\ell$ as the restriction of the map for type B_ℓ. Then $w \in W$ does not commute with any reflection if, and only if,

(i) w^ϕ fixes at most one element of $\{1, \dots, \ell\}$ and, for every transposition (i, j) contained in the cycle decomposition of $\phi(w)$, the cycle occurring in w is $(i, j, -i, -j)$ or $(j, i, -j, -i)$; or
(ii) w^ϕ has exactly two fixed points, say i and j, and the cycle decomposition of w contains $(i, -i)(j)(-j)$ or $(i)(-i)(j, -j)$.

The number of elements of the type (ii) is clearly $\binom{\ell}{2} d_{\ell-2} 2^{\ell-2}(\ell-2)!$, contributing

$$\lim_{\ell\to\infty} \frac{\binom{\ell}{2} 2^{\ell-2} d_{\ell-2}(\ell-2)!}{|W(\mathrm{D}_\ell)|} = \lim_{\ell\to\infty} 2^{-2} d_{\ell-2} = \frac{1}{4e}$$

to the required asymptotic proportion.

Writing T_ℓ for elements of W such that w^ϕ fixes at most two elements and

$$T_\ell^{i,j} = \big\{ w \in T_\ell \;\big|\; w \text{ contains } (i, j)(-i, -j) \text{ or } (i, -j)(j, -i) \big\},$$

we find that the set of elements of type (i) is

$$T_\ell - \bigcup_{1\leqslant i<j\leqslant \ell} T_\ell^{i,j}.$$

Again, we take alternating sums over h-tuples of commuting transpositions in $\phi(W)$. As each transposition in the decomposition of an element of $\phi(w)$ corresponds to two 4-cycles as indicated above, we find the same factor 2^h as for the B_ℓ case:

$$\sum_{h=0}^{\lfloor \ell/2 \rfloor} (-1)^h \binom{\ell}{2h} \frac{(2h)!}{2^h h!} 2^h |T_{\ell-2h}|.$$

As $|T_\ell| = 2^{\ell-1}\ell!(d_\ell + d_{\ell-1})$, the result is

$$\sum_{h=0}^{\lfloor \ell/2 \rfloor} \left(-\frac{1}{4}\right)^h (d_{\ell-2h} + d_{\ell-2h-1}),$$

which contributes

$$\lim_{m\to\infty} \frac{f}{2^\ell \ell!} = \sum_{h=0}^{\infty} \left(-\frac{1}{4}\right)^h \frac{1}{h!}\frac{2}{e} = 2e^{-\frac{1}{4}} e^{-1} = 2e^{-\frac{5}{4}}$$

to the required proportion. Hence, the asymptotic proportion is $(4e)^{-1} + 2e^{-5/4}$.

The exceptional types: These were computed by machine. □

Corollary 6.3 *(Theorem 1.5). The proportion of reflection derangements in a Weyl group is less than* $\frac{2}{3}$.

Proof. Recall that if $a_n > 0$ converges monotonically to zero, then $\sum_{i=0}^{\infty}(-1)^i a_i$ is called an *alternating series*. The maximum value of the partial sums $s_n = \sum_{i=0}^{n}(-1)^i a_i$ of such a series is one of the first two partial sums. Since the series in the proof of the previous proposition are sums of alternating sequences, it is always possible to find a constant M such that the maximum value of the partial sums is one of $s_1, \ldots, s_M$. It is now easy to show on a case-by-case basis that the proportion of reflection derangements in an irreducible Weyl group is at most $\frac{2}{3}$.

If W is a direct product decomposition into s irreducible Weyl groups, then an element of W is a reflection derangement if and only if each component of w is a reflection arrangement, and so their proportion is at most $(\frac{2}{3})^s \leqslant \frac{2}{3}$. □

Together with Proposition 6.1, this shows that the chance of finding a regular semisimple element of L corresponding to a reflection nonderangement in the Weyl group is at least one third, provided q is large enough. To complete the analysis, we need a more precise bound on the probability of finding such regular semisimple elements.

6.3. Bounds on the number of particular semisimple elements

The following useful lemma can be proved by elementary calculus.

Lemma 6.4. *Let $a_1, \ldots, a_m$ be a sequence of nonnegative integers and suppose that no integer appears more than a times in this sequence. Then*

$$\prod_i \left(1 - \frac{1}{q^{a_i}}\right) \geqslant \left(1 - \frac{1}{q}\right)^{2a}.$$

We now start by looking at the Coxeter class in the Weyl group. The Coxeter element is actually a reflection derangement, but this proof is the model for our next result.

Proposition 6.5. *Suppose that W is an irreducible Weyl group. If w_c is a Coxeter element of W, then*

$$\frac{|L_{\mathrm{rss},w_c}(k)|}{|L(k)|} \geqslant \left(1 - \frac{\ell}{q^{\ell/2}}\right)\left(1 - \frac{1}{q}\right)^4 \frac{1}{h},$$

where h is the order of w_c.

Proof. Suppose α is a root and $\alpha {w_c}^m$ is a linear combination of $\alpha, \alpha w_c, \ldots, \alpha {w_c}^{m-1}$. We prove that $m \geqslant \ell/2$ on a case-by-case basis:

Type A_ℓ: Identify W with $\mathrm{Sym}_{\ell+1}$ and consider Φ to consist of roots $e_i - e_j$ with $i \neq j$. We can take $w_c = (1, 2, \ldots, \ell+1)$ and $\alpha = e_i - e_j$. So $\alpha {w_c}^m = e_{i+m} - e_{j+m}$ with the subscripts taken modulo $\ell+1$. Hence $\alpha {w_c}^m$ is a linear combination of $\alpha, \ldots, \alpha {w_c}^m$ iff $i+m$ and $j+m$ are both in $[i, i+m-1] \cup [j, j+m-1]$ modulo $\ell+1$. By the pigeon hole principle, this can only happen if $m \geqslant (\ell+1)/2$.

Type C_ℓ: Identify W with the set of permutations w of $\{\pm 1, \ldots, \pm\ell\}$ such that $(-i)w = -(iw)$ for $i = 1, \ldots, \ell$. Consider $\Phi = \Phi(C_\ell)$ to consist of roots $\varepsilon e_i - \delta e_j$ with $\varepsilon, \delta \in \{\pm 1\}$, $i, j = 1, \ldots, \ell$ and $\varepsilon i \neq \delta j$. We can take

$$w_c = (1, 2, \ldots, \ell, -1, -2, \ldots, -\ell)$$

and $\alpha = \varepsilon e_i - \delta e_j$. The same argument used in type A_ℓ now shows that $m \geqslant \ell/2$.

Table 1
The functions $Q_w(X)$ for a Coxeter element w.

A_ℓ	$\prod_{i=1}^{\ell}(1-X^i)$
B_ℓ, C_ℓ	$(1-X^\ell)\prod_{i=1}^{\ell-1}(1-X^{2i})$
D_ℓ	$\prod_{i\in\{1,\ell-1,\ell\}}(1-X^i)\prod_{i=2}^{\ell-2}(1-X^{2i})$
G_2	$(1-X^2)(1-X^3)(1+X)$
F_4	$(1-X^6)\prod_{i\in\{4,6,8\}}(1-X^i)$
E_6	$(1-X^6)\prod_{i\in\{1,4,5,6,8\}}(1-X^i)(1+X^3+X^6)$
E_7	$(1-X^6)\prod_{i\in\{1,6,8,10,12,14\}}(1-X^i)(1+X^3+X^6)$
E_8	$\prod_{i\in\{1,8,10,12,14,18,20,24\}}(1-X^i)(1+X^3)(1+X^5+X^{10})$

Type B_ℓ: The permutation action of $W(B_\ell)$ on its roots is isomorphic to the action of $W(C_\ell)$ on its roots, so the same argument works.

Types D_ℓ: Identify W with the elements of $W(C_\ell)$ such that $\prod_{i=1}^{\ell}(iw) > 0$ and consider Φ to consist of the roots $\varepsilon e_i - \delta e_j$ with $\varepsilon, \delta \in \{\pm 1\}$, $i, j = 1, \ldots, \ell$ and $i \neq j$. We can take $w_c = (1, 2, \ldots, \ell-1, -1, -2, \ldots, -\ell+1)(\ell, -\ell)$ and $\alpha = \varepsilon e_i - \delta e_j$. Once again $m \geqslant \ell/2$ if $i, j \neq \ell$. If $i = \ell$, $j \neq \ell$, then $\alpha {w_c}^m = (-1)^m \varepsilon e_\ell - \delta e_{j+m}$ with the second subscript taken modulo $\ell - 1$, and so $m \geqslant \ell - 1$.

Exceptional types: These are easily checked by computer.

It is well known that every orbit of w_c on Φ has size h, so $\sum_i c_i(w_c) = 2N/h = \ell$. We have shown that $c_i(w_c) = 0$ for $i < \ell/2$, so

$$1 - \sum_{i=1}^{\ell} \frac{c_i(w_c)}{q^i} \geqslant 1 - \frac{\ell}{q^{\ell/2}}.$$

The functions $Q_{w_c}(X)$ are straightforward to compute and are given in Table 1. The terms in which every coefficient is positive can be ignored, since they are bounded below by 1 when we set $X = 1/q$. Since no term $1 - X^a$ appears more than twice in these polynomials and $q \geqslant 3$, it follows by Lemma 6.4 that $Q_{w_c}(1/q) \geqslant (1 - 1/q)^4$.

The required inequality now follows from the first inequality of Proposition 6.1 and the fact that the centraliser of w_c has order h. □

We now consider reflection nonderangements that are, in some sense, close to being Coxeter elements.

Proposition 6.6. *Suppose that W is an irreducible Weyl group. If W is classical with rank at least 7 then there is a reflection nonderangement w such that*

$$\frac{|L_{\mathrm{rss},w}(k)|}{|L(k)|} \geqslant \left(1 - \frac{3}{q} - \frac{4}{q^2} - \frac{\ell+5}{q^{(\ell-2)/2}}\right)\left(1 - \frac{1}{q}\right)^6 \frac{1}{4\ell}.$$

For other Cartan types there is a reflection nonderangement w such that

$$\frac{|L_{\mathrm{rss},w}(k)|}{|L(k)|} \geqslant \left(1 - \sum_{i=1}^{\ell} \frac{c_i}{q^i}\right)\left(1 - \frac{1}{q}\right)^6 \frac{1}{c}.$$

with the constants c and c_i listed in Table 2.

Table 2
The constants c and c_i for small rank and exceptionals.

Type	c	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
A_1	2	1							
A_2	2	1	2						
B_2, C_2	8	4	0						
G_2	4	3	4						
A_3	8	2	4	0					
B_3, C_3	8	1	2	2					
A_4	6	1	2	0	2				
B_4, C_4	12	1	1	4	0				
D_4	16	5	8	0	0				
F_4	36	3	1	6	0				
A_5	8	1	1	2	4	0			
B_5, C_5	16	1	0	0	4	2			
D_5	16	3	5	2	4	0			
A_6	10	1	0	0	4	0	2		
B_6, C_6	20	1	0	0	2	5	0		
D_6	24	3	5	3	4	0	0		
E_6	36	3	0	3	2	6	0		
E_7	60	3	0	0	2	10	0	0	
E_8	108	3	0	0	0	0	4	9	0

Proof. Fix a root β. Assume β is short (resp. long) for Cartan type B_ℓ (resp. C_ℓ). Let $\Phi_\beta = \{\gamma \in \Phi \mid \langle \gamma, \beta^\star \rangle = 0\}$. Then Φ_β is a subsystem of W and, except in type D_4, it has at most two irreducible components. Let Φ'_β be the irreducible summand of Φ_β of maximal rank. Let s_β be the reflection in β and let w_β be the Coxeter element of $W(\Phi'_\beta)$. We take $w = s_\beta w_\beta$, except for type A_1 where we use $w = 1$, type G_2 where we use $w = s_\beta$, and type D_4 where we use $s_1s_2s_1s_3s_2s_1s_4s_2s_1s_3s_2$. (Here s_i is the ith simple reflection, with the numbering given in [Bou75].) These elements are all reflection nonderangements.

First we prove that

$$\sum_{i=1}^{\ell} \frac{c_i}{q^i} \leqslant \frac{3}{q} + \frac{4}{q^2} + \frac{\ell+5}{q^{(\ell-2)/2}}$$

for the classical types of rank at least 7.

Type A_ℓ: Assume $\beta = e_1 - e_2$. Then Φ_β has type $A_{\ell-2}$, and so orbits within Φ_β contribute at most $\frac{\ell-2}{q^{(\ell-2)/2}}$ to the sum, as in the previous proof. If $\alpha \notin \Phi_\beta$, then $\alpha = \pm(e_i - e_j)$ where $i = 1$ or 2 and $j > 2$. These roots form one orbit of size 2 and either two orbits of size $\ell - 1$ or one orbit of size $2(\ell - 1)$. So these orbits contribute at most $1/q + 2/q^\ell$.

Type B_ℓ *with* β *short*: Assume $\beta = e_1 - e_2$. Then Φ_β has type $B_{\ell-1}$, and so the orbits within Φ_β contribute at most $\frac{\ell-1}{q^{(\ell-1)/2}}$. If $\alpha \notin \Phi_\beta$, then $\alpha = \varepsilon e_i - \delta e_j$ where $i = 1$ or 2 and $j > 2$. These roots form four orbits of size two with $m = 1$ and four orbits with $m = \ell - 2$.

Type C_ℓ *with* β *long*: This is similar to type B_ℓ, with the short roots and long roots exchanged.

Type D_ℓ: Assume $\beta = e_1 - e_2$. Then Φ_β has type $D_{\ell-2}A_1$ and Φ'_β is the subsystem of type $D_{\ell-2}$. So the orbits within Φ'_β contribute at most $\frac{\ell-2}{q^{(\ell-1)/2}}$ to the sum. If $\alpha \notin \Phi'_\beta$, then $\alpha = \varepsilon e_i - \delta e_j$ where $i = 1$ or 2 and $j > 2$. These roots form at most four orbits with $m = \ell - 2$.

The values of the constants in Table 2 are easily computed in Magma [BC97]. The constant c is just $|C_W(w)|$. The functions $Q_w(X)$ are given in Table 3. Applying Lemma 6.4, we get $Q_w(1/q) \geqslant (1 - 1/q)^6$.

Table 3
The functions $Q_w(X)$.

A_1	$1-X$
A_2	$1-X^3$
A_3	$(1-X)(1-X^3)(1+X^2)$
A_ℓ $(\ell>3)$	$\prod_{i\in\{1,\dots,\ell+1\}\setminus\{2,\ell-1\}}(1-X^i)$
B_2, C_2	$(1-X)^2(1+X^2)$
B_3, C_3	$(1-X)(1-X^2)(1-X^6)$
B_4, C_4	$(1-X)(1-X^3)(1-X^4)(1-X^8)$
B_ℓ, C_ℓ $(\ell>4)$	$(1-X)(1-X^{\ell-2})^{(3-(-1)^\ell)/2}\prod_{i\in\{2,\dots,\ell\}\setminus\{\ell-1\}}(1-X^{2i})$
D_4	$(1-X)^2(1+X^6)(1+X^2)^2$
D_5	$(1-X)^3(1-X^5)(1-X^6)(1+X^2)(1+X^4)$
D_6	$(1-X)^3(1-X^3)(1-X^6)(1-X^{10})(1+X^2)^2(1+X^4)$
D_ℓ $(\ell>6)$	$(1-X)^3\prod_{i\in\{\ell-3,\ell\}}(1-X^i)\prod_{i\in\{4,\dots,\ell-1\}\setminus\{\ell-3\}}(1-X^{2i})(1+X^2)(1+X^2+X^4)$
G_2	$1-X^6$
F_4	$\prod_{i\in\{1,3,8,12\}}(1-X^i)$
E_6	$(1-X)^2\prod_{i\in\{5,8,9,12\}}(1-X^i)$
E_7	$(1-X)^2\prod_{i\in\{5,6,12,14,18\}}(1-X^i)(1+X^2)(1+X^4)$
E_8	$(1-X)^2\prod_{i\in\{6,12,14,20,24,30\}}(1-X^i)(1+X^2)(1+X^4)(1+X^3+X^6)$

For groups not covered in Table 2, let h_β be the Coxeter number of Φ'_β. Then the centraliser of w_β in $W(\Phi'_\beta)$ has order h_β, and the centraliser of w in W has order $2h_\beta \leqslant 4\ell$. The required result now follows from the first inequality of Proposition 6.1. □

6.4. Time analysis

Finally we are in a position to give an analysis of Algorithm 8, which searches for a split maximal toral subalgebra.

As discussed in Section 6.2, the probability of finding f with $\deg(f)=1$, or with $\deg(f)=2$ and $f=f_-$, is bounded below by the chance of the corresponding Weyl group element being a reflection nonderangement.

The following result immediately implies Theorem 1.4.

Theorem 6.7. *Suppose that the characteristic of k is greater than 3. Let G be a k-split connected reductive group and let L be the Lie algebra of G. We can find a split maximal toral subalgebra of L in Las Vegas time $O^\sim(n^3\ell^6\log(q)^2)$.*

Proof. Before calling Algorithm 8, we compute the centre $Z(L)$ of L, which takes time $O^\sim((n+\ell^2)^3\log(q))$.

Algorithm 8 begins by calling Algorithm 5 which takes the time of computing the centraliser of an element x and the computation of the minimal polynomial of $\mathrm{ad}(x)$, all of which is bounded by $O^\sim(n^3\log(q)^2)$. Also, testing whether a maximal toral subalgebra H/Z is split and finding the generalised roots of L/Z with respect to H/Z can be computed in $O^\sim(\ell^7\log(q)^2)$. In view of Lemma 5.7, the computation time for M/Z and K/Z in each of the cases is also bounded from above by this estimate. We conclude that the computations within the main loop take time $O^\sim(\ell^7\log(q)^2)$.

Therefore, the critical time estimate hinges on the probability of finding a suitable maximal toral subalgebra, that is, the centraliser of an element of $L_{\mathrm{rss},w}(k)$ for w a reflection nonderangement. A lower bound on the ratio $|L_{\mathrm{rss},w}(k)|/|L(k)|$ can be obtained by consideration of a single component of Φ, so, for the remainder of the time analysis we can assume, without loss of generality, that Φ is irreducible.

By Proposition 6.6, if G is classical with rank at least 7, we obtain a split toral subalgebra in L/Z of rank at least 1 with probability at least

$$\left(1-\frac{1}{q}\right)^6\left(1-\frac{3}{q}-\frac{4}{q^2}-\frac{\ell+5}{q^{(\ell-2)/2}}\right)\frac{1}{4\ell}.$$

For $q \geqslant 5$ and $\ell \geqslant 7$, this is at least

$$\left(\frac{4}{5}\right)^6\left(1-\frac{3}{5}-\frac{4}{25}-\frac{12}{5^{5/2}}\right)\frac{1}{4\ell} > 0.$$

Similarly for the Cartan types in Table 2, except for D_4,

$$\left(1-\sum_{i=1}\frac{c_i}{q^i}\right)\left(1-\frac{1}{q}\right)^6\frac{1}{c} \geqslant \left(1-\sum_{i=1}\frac{c_i}{5^i}\right)\left(1-\frac{1}{5}\right)^6\frac{1}{c} > 0.$$

For type D_4, the bound is negative for $q = 5$, but positive for $q \geqslant 7$. So it remains to consider the Lie algebra $D_4(5)$. But for any fixed Lie algebra, it is easily seen that there is a nonzero chance of the algorithm working, since there is a fixed positive lower bound on the probability that the toral subalgebra found by Algorithm 5 is already split. Therefore, we have shown that there is a constant $C > 0$ such that the probability of success after one iteration of the main loop is at least C/ℓ.

Since

$$\lim_{\ell\to\infty}\left(1-\frac{C}{\ell}\right)^{a\ell} = e^{-aC},$$

we can choose a such that

$$\left(1-\frac{C}{\ell}\right)^{a\ell} \leqslant \frac{1}{e^4}$$

for all ℓ. Hence the probability of failure after $a\ell\log(\ell)$ repetitions of the loop is at most

$$\left(1-\frac{C}{\ell}\right)^{a\ell\log(\ell)} \leqslant \left(\frac{1}{e^4}\right)^{\log(\ell)} = \frac{1}{\ell^4}.$$

Clearly the depth of recursion is at most ℓ, which contributes a further factor of ℓ to our timing, so the total number of recursive calls is at most $\ell^2\log(\ell)$. Hence the overall probability of success is at least

$$\left(1-\frac{1}{\ell^4}\right)^{\ell^2\log(l)} \geqslant \frac{1}{2}.$$

Hence Algorithm 8 takes Las Vegas time $O^\sim(\ell^9\log(q)^2)$. Combining this with the preprocessing time of $O^\sim((n+\ell^2)^3\log(q))$, and using the fact that $n \geqslant \ell$ we get the desired result. □

Corollary 6.8. *Suppose that the characteristic of k is greater than 3. Let G be a k-split connected reductive group and let L be the Lie algebra of G. We can find a Chevalley basis of L in Las Vegas time $O^\sim(n^3\ell^6\log(q)^2)$.*

Proof. The time taken to find a split maximal toral subalgebra clearly dominates the time for Algorithm 9, which is dealt with in Theorem 6.7. □

Hence, combining this corollary with Lemma 5.9 and Proposition 4.4, we see that the algorithm for Lang's Theorem takes time

$$O^{\sim}\big(n^3\ell^6\log(q)^2 + n^6m^2r^2s^2\log(q)^2\big),$$

which easily leads to the timing in Theorem 1.2.

References

[Bab97] László Babai, Randomization in group algorithms: Conceptual questions, in: Groups and Computation, II, New Brunswick, NJ, 1995, Amer. Math. Soc., Providence, RI, 1997, pp. 1–17.

[BC97] W.W. Bosma, J.J. Cannon, Handbook of Magma Functions, School of Mathematics and Statistics, University of Sydney, Sydney, 1997.

[Bou75] N. Bourbaki, Éléments de mathématique, Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées, Actualités Scientifiques et Industrielles, No. 1364, Hermann, Paris, 1975.

[Car72] Roger W. Carter, Simple Groups of Lie Type, Pure Appl. Math., vol. 28, John Wiley & Sons, London, 1972.

[Car93] Roger W. Carter, Finite Groups of Lie Type: Conjugacy Classes and Complex Characters, John Wiley & Sons, Chichester, 1993, reprint of the 1985 original, Wiley–Interscience Publication.

[CHM08] Arjeh M. Cohen, Sergei Haller, Scott H. Murray, Computing in unipotent and reductive algebraic groups, LMS J. Comput. Math. 11 (2008) 343–366.

[CLG97] Frank Celler, C.R. Leedham-Green, Calculating the order of an invertible matrix, in: Groups and Computation, II, New Brunswick, NJ, 1995, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 55–60.

[CMT04] Arjeh M. Cohen, Scott H. Murray, D.E. Taylor, Computing in groups of Lie type, Math. Comp. 73 (2004) 1477–1498.

[Dem65] M. Demazure, Données radicielles, in: Schémas en Groupes, Sém. Géométrie Algébrique, Fasc. 6, Exposé 21, Inst. Hautes Études Sci., 1964, Inst. Hautes Études Sci., Paris, 1965.

[dG00] Willem A. de Graaf, Lie Algebras: Theory and Algorithms, North-Holland Publishing Co., Amsterdam, 2000.

[dGIR96] Willem A. de Graaf, Gábor Ivanyos, Lajos Rónyai, Computing Cartan subalgebras of Lie algebras, Appl. Algebra Engrg. Comm. Comput. 7 (5) (1996) 339–349.

[GH97] S.P. Glasby, R.B. Howlett, Writing representations over minimal fields, Comm. Algebra 25 (6) (1997) 1703–1711.

[Gro02] Larry C. Grove, Classical Groups and Geometric Algebra, Grad. Stud. Math., vol. 39, Amer. Math. Soc., Providence, RI, 2002.

[Hog82] G.M.D. Hogeweij, Almost-classical Lie algebras. I, II, Indag. Math. (N.S.) 44 (4) (1982) 441–452, 453–460.

[Hum67] James E. Humphreys, Algebraic groups and modular Lie algebras, Mem. Amer. Math. Soc. 71 (1967).

[Hum75] James E. Humphreys, Linear Algebraic Groups, Grad. Texts in Math., vol. 21, Springer-Verlag, New York, 1975.

[Hum78] James E. Humphreys, Introduction to Lie Algebras and Representation Theory, Springer-Verlag, New York, 1978 (second printing, revised).

[Jac62] Nathan Jacobson, Lie Algebras, Interscience Tracts Pure Appl. Math., vol. 10, Interscience Publishers, New York, 1962.

[Leh92] G.I. Lehrer, Rational tori, semisimple orbits and the topology of hyperplane complements, Comment. Math. Helv. 67 (2) (1992) 226–251.

[Leh98] G.I. Lehrer, The cohomology of the regular semisimple variety, J. Algebra 199 (2) (1998) 666–689.

[LN97] Rudolf Lidl, Harald Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997 (with a foreword by P.M. Cohn).

[Mül03] Peter Müller, Algebraic groups over finite fields, a quick proof of Lang's theorem, Proc. Amer. Math. Soc. 131 (2003) 369–370 (electronic).

[Ryb07] Alexander J.E. Ryba, Identification of matrix generators of a Chevalley group, J. Algebra 309 (2) (2007) 484–496.

[Sel67] George B. Seligman, Some results on Lie p-algebras, Bull. Amer. Math. Soc. 73 (1967) 528–530.

[Shp99] Igor E. Shparlinski, Finite fields: Theory and computation, in: The Meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography, in: Math. Appl., vol. 477, Kluwer Academic Publishers, Dordrecht, 1999.

[Spr98] T.A. Springer, Linear Algebraic Groups, second ed., Birkhäuser Boston Inc., Boston, MA, 1998.

[SV00] Tonny A. Springer, Ferdinand D. Veldkamp, Octonions, Jordan Algebras and Exceptional Groups, Springer Monogr. Math., Springer-Verlag, Berlin, 2000.

[vzGS92] Joachim von zur Gathen, Victor Shoup, Computing Frobenius maps and factoring polynomials, Comput. Complexity 2 (3) (1992) 187–224.